

Vigor2950 系列
雙 WAN 口防火牆
使用手冊

版本: **1.0**

日期: **2007/01/16**

因手冊更新無法及時通知用戶，請隨時連上居易網站，取得最新的手冊內容。

安全說明和保障

安全說明

- 在設置前請先閱讀安裝說明。
- 由於路由器是複雜的電子產品，請勿自行拆除或是維修本產品。
- 請勿自行打開或修復路由器。
- 請勿把路由器置於潮濕的環境中，例如浴室。
- 請將本產品放置在足以遮風避雨之處，適合溫度在攝氏 5 度到 40 度之間。
- 請勿將本產品暴露在陽光或是其他熱源下，否則外殼以及零件可能遭到破壞。
- 請勿將 LAN 纜線置於戶外，以防電擊危險。
- 請將本產品放置在小孩無法觸及之處。
- 若您想棄置本產品時，請遵守當地的保護環境的法律法規。

保固

自使用者購買日起二年內為保固期限，請將您的購買收據保存二年，因為它可以證明您的購買日期。當本產品發生故障乃導因於製作及(或)零件上的錯誤，只要使用者在保固期間內出示購買證明，居易科技將採取可使產品恢復正常之修理或更換有瑕疵的產品(或零件)，且不收取任何費用。居易科技可自行決定使用全新的或是同等價值且功能相當的再製產品。

下列狀況不在本產品的保固範圍內：(1)若產品遭修改、錯誤(不當)使用、不可抗力之外力損害，或不正常的使用，而發生的故障；(2) 隨附軟體或是其他供應商提供的授權軟體；(3) 未嚴重影響產品堪用性的瑕疵。

成為一個註冊用戶

建議在 Web 介面進行註冊。您可以到 http://www.draytek.com.tw 註冊您的 Vigor 路由器。

韌體及工具的更新

請造訪 DrayTek 主頁以獲取有關最新韌體、工具及檔案文件的資訊。
http://www.draytek.com.tw

歐盟聲明

廠商: 居易科技股份有限公司
地址: 臺灣新竹工業區湖口鄉復興路 26 號
產品: VigorPro 5500

DrayTek 公司聲明 VigorPro 5500 服從以下基本要求以及其他 R&TTE 指令（1999/5/EEC）的相關規定。

產品根據 EN55022/Class A 以及 EN55024/Class A 規範，遵從電磁相容性（EMC）指令 89/336/EEC。

產品根據 EN60950 規範，遵從低壓（LVD）73/23/EEC 的要求。

法規資訊

聯邦通信委員會干擾聲明

此設備經測試，依照 FCC 規定第 15 章，符合 A 級數位器件的限制標準。這些限制是爲居住環境不受有害的干擾，而提供合理的保護。若沒有按指導進行安裝和使用，此器件生成、使用以及發射出的無線電能量可能會對無線電通訊有害的干擾。然而，我們並不保證在特殊安裝下，不會產生干擾。如果此產品確實對無線電或電視接受造成了有害的干擾（可以透過開關路由器來判定），我們建議用戶按照以下的幾種方法之一來解決干擾：

- 重新調整或定位接收天線。
- 增加設備和接受器之間的間隔。
- 將設備接到一個與接受者不同的回路的出口。
- 請代理商或是有經驗的無線電/電視技師協助處理。

此產品符合 FCC 規定的第 15 部分。其運作將有以下兩個情況：

(1) 此產品不會造成有害的干擾，並且

(2) 此產品可能會遭受其他接收到的干擾，包括那些可能造成不良運作的干擾。

請造訪 www.draytek.com/about_us/Regulatory.php.



本產品針對 2.4 GHz 無線網路而設計，適用範圍遍及歐洲共同體及瑞士，法國地區則有部分的限制。



這是 A 級產品，在家用的環境當中，本產品可能引起居住環境中的無線電信號干擾。在此情況下，用戶可能需要適當地調整一下使用策略。

目錄

1 前言

Vigor2950 系列路由器針對網際網路存取動作，提供雙 WAN 介面(第二組 WAN 設定是可調式的) 以便讓網際網路連線更安全可靠。無線區域網路支援 108Mbps (SuperG^{TM}) 傳輸速度 108Mbps 及更多的安全性功能，物件導向防火牆非常有彈性，而且可使您的網路環境更加安全。

1.1 網頁設定按鈕說明

在路由器的網頁設定中，有數種常見的按鈕，其定義如下所示：

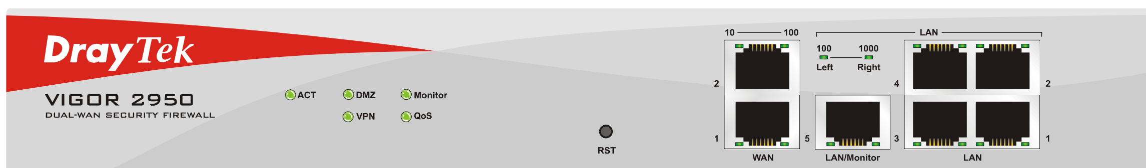
按鈕	說明
確定	儲存並套用目前的設定。
取消	取消目前設定並回復先前的設定值。
清除	捨棄目前設定值並允許使用者重新輸入。
新增	指定項目新增設定。
編輯	編輯選定項目的設定。
刪除	刪除選定項目及相關設定。

附註:有關網頁上所出現的其他按鈕，請參考第四章。

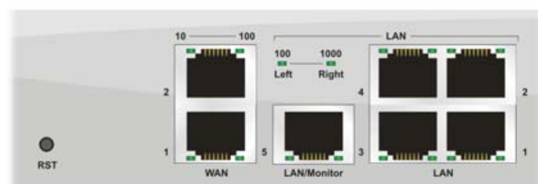
1.2 LED 指示燈與介面說明

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

1.2.1 Vigor2950



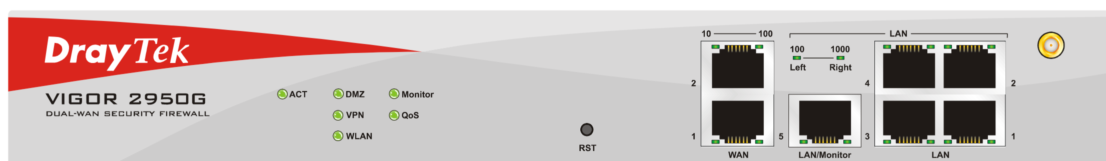
LED		狀態	說明
ACT (活動)		閃爍	路由器已開機並可正常運作。
		暗	路由器已關機。
DMZ		亮	於特定位置指定 DMZ 主機。
VPN		亮	VPN 通道已建立。
		暗	VPN 通道已關閉。
Monitor		亮	啓動 LAN 資料傳輸監視動作。
QoS		亮	QoS 功能已開啓。
連接介面上的LED 燈號			
WAN	10 (左 LED)	亮	介面的連接速度是正常的 10Mbps。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	100 (右 LED)	亮	介面的連接速度是正常的 100Mbps。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
LAN/Monitor LAN	100 (左 LED)	亮	介面的連接速度是正常的 100Mbps。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	1000 (右 LED)	亮	介面的連接速度是正常的 1000Mbps。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。





介面	說明
RST (出廠預設值按鈕))	恢復預設設定 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
WAN(1/2)	連接到 Internet（網際網路）的介面。
LAN/Monitor	連接到本地網路的介面。
LAN (1-4)	連接到本地網路的介面。
	電源介面 100-240VAC。
	電源開關，“1” 爲開，“0” 爲關。

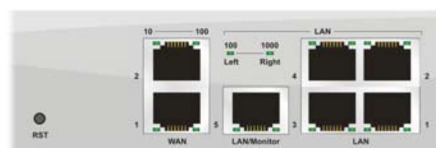
1.2.2 Vigor2950G



LED	狀態	說明
ACT (活動)	閃爍	路由器已開機並可正常運作。
	暗	路由器已關機。
DMZ	亮	於特定位置指定 DMZ 主機。
VPN	亮	VPN 通道已建立。
	暗	VPN 通道已關閉。
WLAN	亮	無線 AP 預備妥當可以使用。
	閃爍	資料封包透過無線網路傳輸中。
	暗	無線網路功能無法使用。
Monitor	亮	啟動 LAN 資料傳輸監視動作。
QoS	亮	QoS 功能已開啓。

連接介面上的LED 燈號

WAN	10 (左 LED)	亮	介面的連接速度是正常的 10Mbps。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	100 (右 LED)	亮	介面的連接速度是正常的 100Mbps。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
LAN/Monitor LAN	100 (左 LED)	亮	介面的連接速度是正常的 100Mbps。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	1000 (右 LED)	亮	介面的連接速度是正常的 1000Mbps。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。





介面	說明
RST (出廠預設值按鈕)	恢復預設設定 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
WAN(1/2)	連接到 Internet（網際網路）的介面。
LAN/Monitor	連接到本地網路的介面。
LAN (1-4)	連接到本地網路的介面。
	電源介面 100-240VAC。
	電源開關，“1” 為開，“0” 為關。

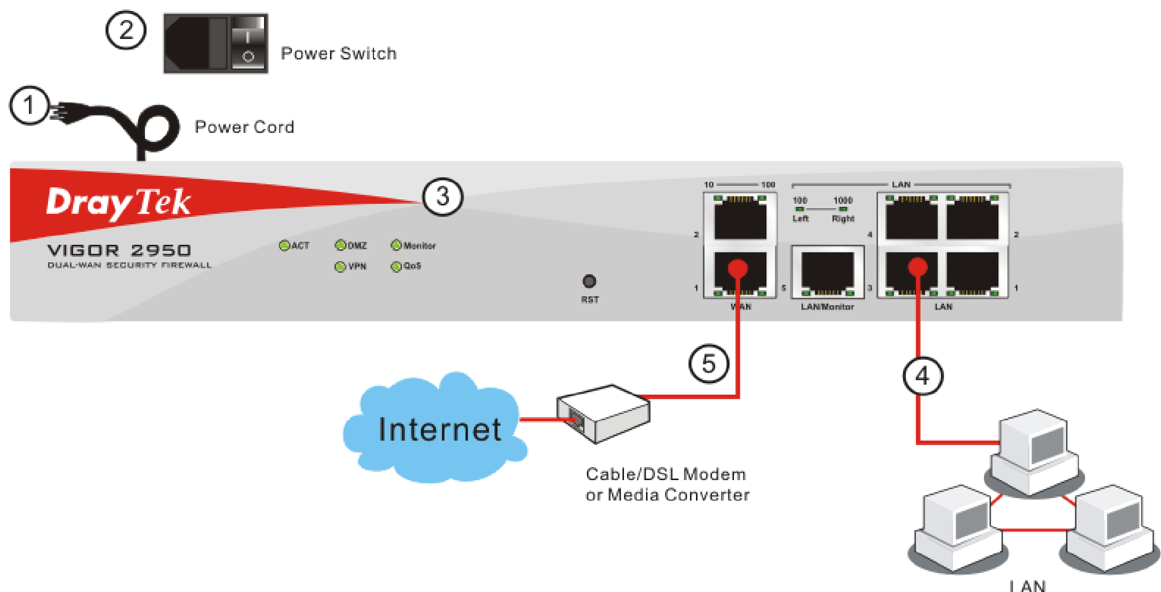
1.3 安裝您的路由器

此章節將指導您如何安裝路由器的硬體部分，以及如何從 web 瀏覽器設定路由器。

在使用路由器之前，您需要正確地連接您的設備。

1. 將電源線連接到路由器背面板的電源插口，另一端連接到牆上電源輸出孔。
2. 按下面板背面的電源開關，開啓路由器。
3. 系統開始運作，在完成自我檢測後，**ACT** LED 開始閃爍。
4. 將乙太網路纜線(RJ-45)一端連接 PC 的乙太網路連接埠，一端連接到路由器任何一個 **LAN** 連接埠，相對應的 **LAN** LED 將依據網路卡的種類及設定(100Mbps 或 10Mbps)而決定亮燈(左邊或右邊燈)。
5. 依照實際的需要，利用乙太網路纜線(RJ-45)將數據機/路由器連接到本裝置的 WAN 連接埠，相對應的 **WAN1/WAN2** LED(左邊或右邊燈)將依據網路卡的種類及設定(100Mbps 或 10Mbps)而決定亮燈。

(有關 LED 狀態的詳細資訊請參考章節 1.1。)



(有關 LED 狀態的詳細資訊請參考章節 1.1。)

2 基本設定

在開始使用路由器時，基於安全的考量，我們強烈建議你在路由器上設定一組管理者密碼。路由器的出廠設定是沒有密碼的。如果不設定密碼，路由器可能被 LAN 或 Internet 上的任何使用者登入並且變更設定而導致您的資料流失。在此章節我們會為您介紹下列幾項基本設定功能：快速設定精靈，系統管理員密碼設定，以及區域網路 TCP/IP 與 DHCP 設定。

2.1 變更密碼

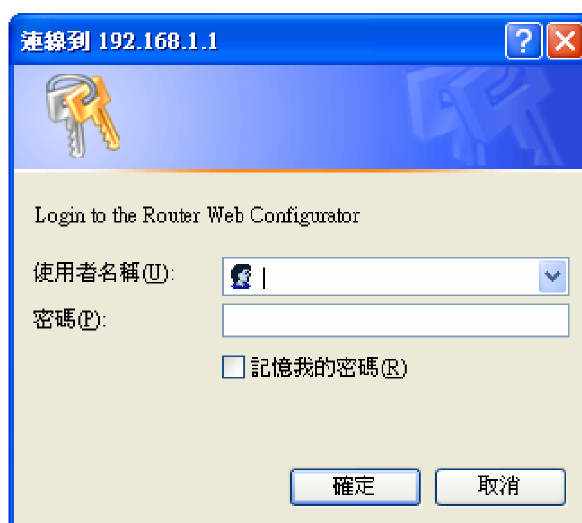
如要變更此裝置的密碼，您必須以預設的密碼先進入網頁。

1. 確保您的電腦已經和路由器正確的連接。



附註: 您可以選擇直接設定電腦的網路設定為動態取得 IP 位址 (DHCP)，或者是將 IP 設定為和 IP 分享器的預設 IP 位址 (192.168.1.1) 於同一個子網路。如需更多訊息，請參考後面的章節 – 疑難排解。

2. 開啓網頁瀏覽器並輸入位址 http://192.168.1.1。將會出現登入視窗。因為這是您第一次進入設定介面，請輸入預設的系統管理員名稱及密碼預設值 (預設為空值，也就是將欄位留著空白)，並按確定進入設定介面。



3. 現在，設定介面的主選單會出現。



注意： 因爲首頁會依照您的路由器的功能而有些微改變，所以設定介面不一定都會如上圖所示。

4. 進入**系統維護**頁面並選擇**系統管理員密碼**。

系統維護 >> 系統管理員密碼設定

系統管理員密碼

舊密碼	
新密碼	
確認密碼	

確定

5. 輸入舊密碼 (預設值爲空白)。 在**新密碼**及**確認密碼**輸入您想要設定的密碼，然後按**確定**儲存設定。

6.　現在您已經完成變更密碼設定。請記得在下一次登入設定介面時使用新的密碼。



2.2 快速設定精靈

如果您打算佈建此路由器在現成的高速 NAT 網路結構中，您可以依照下列的步驟使用快速設定精靈設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按下一步。

快速設定精靈

輸入登入密碼

請重新輸入字母及數字組合之字串作為您的 **密碼** (最多23個字元).

新密碼

確認密碼

< 上一步　下一步 >　完成　取消

在如下的頁面中，請選擇 WAN 介面，挑選**自動偵測**作爲連線模式，然後按**下一步**。

快速設定精靈

選擇 WAN 介面

選擇 WAN 介面: WAN1
顯示名稱:
實體模式: 乙太網路
連線模式: 自動偵測
自動偵測
10M 半雙工
10M 全雙工
100M 半雙工
100M 全雙工

<上一步 下一步> 完成 取消

在下圖顯示中，請依照您的 ISP 提供的資料，選擇適當的網際網路連線類型，例如 ISP 提供您 PPPoE 介面的資訊，您就應該選擇 PPPoE 模式。接著按下一步進行。

快速設定精靈

連線至網際網路

WAN 1
從下列網際網路連線方式類型中，選擇您的網路供應商所提供的服務類型，如果您不確定應該選擇何種類型，請聯繫您的網路服務供應商以取得詳細資料。

- PPPoE
- PPTP
- 固定 IP
- DHCP

<上一步 下一步> 完成 取消

在快速設定精靈中，您可以設定路由器的網路連線設定如 PPPoE、PPPTP、固定 IP、DHCP。針對網際網路連線動作，路由器提供 DSL WAN 介面給用戶選擇。

2.2.1 PPPoE

PPPoE 爲 Point-to-Point Protocol over Ethernet 的縮寫，是一種利用個人電腦透過寬頻連接設備(如 xDSL、Cable、Wireless)連接至高速寬頻網路的技術，用戶僅需在個人的電腦上加裝乙太網路卡，然後向電信線路提供者(如：中華電信)與網際網路服務提供者(ISP，如：亞太線上)申請 ADSL 服務，就可以以類似傳統撥接的方式，透過一般的電話線連上網際網路。另外，PPPoE 也同時被用來在 ADSL 網路架構上進行用戶認證、紀錄用戶連線時間，以及取得動態 IP。

如果您的 ISP 業者提供您 PPPoE 連線方式， 請先在視窗中選擇適當的模式，然後輸入相關資訊：

快速設定精靈

PPPoE 用戶端模式

WAN 1

請輸入您的網路服務供應商所提供的使用者名稱及密碼。

使用者名稱	84005765@hinet.net
密碼	●●●●●●●●●
確認密碼	●●●●●●●●●

<上一步 下一步> 完成 取消

使用者名稱　　指定 ISP 提供之有效使用者名稱。

密碼　　指定 ISP 提供之有效密碼。

確認密碼　　重新輸入密碼以確認。

按下一步檢視此連線的設定狀態。

快速設定精靈

請確認您的設定:

WAN 介面:	WAN1
實體模式:	乙太網路
連線模式:	自動偵測
網際網路連線:	PPPoE

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

<上一步 下一步> 完成 取消

按完成，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

快速設定精靈設定完成!!!

2.2.2 PPTP

PPTP 則是 Point-to-Point Tunneling Protocol 的簡稱。有些 DSL 服務提供者採用一種特別的 DSL 數據機(例如：阿爾卡特的 DSL 數據機)。這種數據機只支援 PPTP Tunnel 方法存取 Internet。在這種情形下，您建立一個到 DSL 數據機並且帶有 PPP Session 的 PPTP Tunnel。一但 Tunnel 建立後，這種 DSL 數據機會將 PPP Session 送往 ISP。當 PPP Session 建立後，當地的使用者共用這個 PPP Session 存取網際網路。如果您需要使用 PPPTP 連線，請先在視窗中選擇適當的模式，然後輸入相關資訊：

快速設定精靈

PPTP 用戶端模式

WAN 1

請輸入您的網路服務供應商所提供的使用者名稱、密碼、WAN IP 組態設定及PPTP 伺服器IP。

使用者名稱	admin
密碼	●●●●●
確認密碼	●●●●●
WAN IP 組態設定	
○ 自動取得IP 位址	
◉ 指定IP 位址	
IP 位址	172.16.3.229
子網路遮罩	255.255.0.0
PPTP 伺服器 IP	

<上一步 | 下一步> | 完成 | 取消

按下一步檢視此連線的設定狀態。

快速設定精靈

請確認您的設定:

WAN 介面:	WAN1
實體模式:	乙太網路
連線模式:	自動偵測
網際網路連線:	PPTP

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

<上一步 | 下一步 > | 完成 | 取消

按完成，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

快速設定精靈設定完成!!!

2.2.3 固定 IP

在這種應用當中,您會從 ISP 取得一個固定真實 IP 位址或一個真實子網路(多個公開 IP 位址)。通常纜線(Cable) ISP 會提供一個固定的真實 IP，而 DSL ISP 則有可能會提供一個真實子網路。如果您擁有一個真實子網路，您可以選擇一個或多個 IP 位址設定在 WAN 介面。如果您需要使用固定 IP / 動態 IP，請先在視窗中選擇適當的模式，然後輸入相關資訊：

快速設定精靈

固定 IP 用戶端模式

WAN 1

請輸入您的網路服務供應商所提供的固定 IP 組態設定。

WAN IP	172.16.3.229
子網路遮罩	255.255.0.0
閘道	172.16.3.4
主要 DNS	
次要 DNS	(視需要填入)

<上一步 | 下一步 > | 完成 | 取消

設定輸入完畢之後，按下一步檢視此連線的設定狀態。

快速設定精靈

請確認您的設定:

WAN 介面:	WAN1
實體模式:	乙太網路
連線模式:	自動偵測
網際網路連線:	固定 IP

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

<上一步 | 下一步 > | 完成 | 取消

按完成，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

快速設定精靈設定完成!!!

2.2.4 DHCP

選擇 **DHCP** 作爲通訊協定，並在頁面上輸入 ISP 提供給您的全部訊息。

快速設定精靈

DHCP 用戶端模式

WAN 1

如果您的網路服務供應商要求您輸入特定的主機名稱或特定的MAC位址，請在此輸入。

主機名稱	(視需要填入)
MAC	00 - 50 - 7F - C0 - 2F - F5 (視需要填入)

< 上一步　下一步 >　完成　取消

設定輸入完畢之後，按下一步檢視此連線的設定狀態。

快速設定精靈

請確認您的設定:

WAN 介面:	WAN1
實體模式:	Ethernet
連線模式:	自動偵測
網際網路連線:	DHCP

按 上一步 修正內容，否則請按 完成 儲存目前設定並重新啟動路由器

< 上一步　下一步 >　完成　取消

按完成，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

快速設定精靈設定完成!!!

2.3 線上狀態

線上狀態顯示出系統目前執行的情形，WAN 連接狀況，ADSL 資訊和其他與路由器有關的訊息。

PPPoE (用於 WAN2)

連線狀態

連線狀態　　已開機時間: 18:30:39

區域網路狀態		主要 DNS: 194.109.6.66	次要 DNS: 168.95.1.1
IP 位址	傳送封包	接收封包	
192.168.1.1	22079	12171	

WAN 1 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		固定 IP	18:30:32	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
172.16.3.229	172.16.3.4	9568	5	490353	2733

WAN 2 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		PPPoE	0:00:00	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
61.230.209.207	61.230.192.254	10	16	10	12

固定 **IP (用於 WAN1)**

連線狀態

連線狀態　　已開機時間: 18:30:39

區域網路狀態		主要 DNS: 194.109.6.66	次要 DNS: 168.95.1.1
IP 位址	傳送封包	接收封包	
192.168.1.1	22079	12171	

WAN 1 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		固定 IP	18:30:32	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
172.16.3.229	172.16.3.4	9568	5	490353	2733

WAN 2 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		PPPoE	0:00:00	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
61.230.209.207	61.230.192.254	10	16	10	12

DHCP (用於 WAN1)

連線狀態

連線狀態 已開機時間: 18:30:39

區域網路狀態		主要 DNS: 168.95.1.1		次要 DNS: 139.175.252.16	
IP 位址	傳送封包	接收封包			
192.168.1.1	22079	12171			
WAN 1 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		DHCP Client	0:00:03	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
202.211.100.58	202.211.100.1	2	9	2	94
WAN 2 狀態					
啟用	實體模式	顯示名稱	模式	連線時間	
是	乙太網路		PPPoE	0:00:00	
IP	閘道 IP	傳送封包	傳送速率	接收封包	接收速率
61.230.209.207	61.230.192.254	10	16	10	12

詳細說明於後：

主要 **DNS**	顯示主要 DNS 的 IP 位址。
次要 **DNS**	顯示次要 DNS 的 IP 位址。
區域網路狀態	
IP 位址	顯示區域網路介面的 IP 位址。
傳送封包	顯示在區域路中全部的傳送封包量。
接收封包	顯區域路中全部的接收封包量。
WAN1/2 狀態	
實體模式	顯示實體介面連線的狀態。
顯示名稱	顯示 WAN1/WAN 網頁上所顯示的名稱。
模式	顯示 WAN 連接(PPPoE)的類型。
連線時間	顯示介面上全部的上傳時間。
IP	顯示 WAN 介面的 IP 位址。
閘道 **IP**	顯示預設閘道的 IP 位址。
傳送封包	顯示 WAN 介面上全部傳送的封包數。
傳送速率	顯示 WAN 介面上全部傳送速率位元數。
接收封包	顯示 WAN 介面上全部接收的封包數。
接收速率	顯示 WAN 介面上全部接收速率位元數。

注意**:**綠色字樣表示該 WAN 連接已預備妥當，隨時可以存取網際網路資料，紅色字樣則表示該 WAN 連接尚未預備妥當，也還無法透過路由器存取網際網路資料。

2.4 儲存設定

每當您按下網頁上的確定按鈕以儲存檔案，您都可以見到如下的訊息，此爲系統提供的狀態通知。



預備表示系統處於預備狀態隨時可以輸入設定。

設定已儲存表示您按了完成或是確定按鈕之後，系統已儲存該設定

本頁留白供註解使用

3 進階設定

在您完成基本路由器設定之後，您就可以輕輕鬆鬆的進出網際網路了！不過，針對個人特殊需要，系統提供給您更多的進階設定，至於其他應用範例部份，煩請參考第四章。

3.1 WAN

快速安裝精靈提供使用者一個簡單的方法，以便能快速設定路由器的連線模式。如果您想要針對不同廣域網路模式調整更多的設定，請前往 **WAN** 群組然後點選**網際網路連線控制**連結。本節將會為您介紹一些網際網路的基本觀念，並詳細說明所有的連線模式。

3.1.1 IP 網路的基本概念

IP 表示網際網路通訊協定，在以 IP 為主的網路像是路由器、列印伺服器和主機電腦的每一種裝置，都需要一組 IP 位址作為網路上身分辨識之用。為了避免位址產生衝突，IP 位址都必須於網路資訊中心(NIC) 公開註冊，擁有個別 IP 位址對那些於真實網路分享的裝置是非常必要的，但在虛擬網路上像是路由器所掌管下的主機電腦就不是如此，因為它們不需要讓外人從真實地區進入存取資料。因此 NIC 保留一些永遠不被註冊的特定位址，這些被稱之為虛擬 IP 位址，範圍條列如下：

從 **10.0.0.0** 到 **10.255.255.255**
從 **172.16.0.0** 到 **172.31.255.255**
從 **192.168.0.0** 到 **192.168.255.255**

什麼是真實 IP 位址和虛擬 IP 位址

由於路由器扮演著管理及保護其區域網路的角色，因此它可讓主機群間互相聯繫。每台主機都有虛擬 IP 位址，是由路由器的 DHCP 伺服器所指派，路由器本身也會使用預設之虛擬 IP 位址 192.168.1.1 與本地主機達成聯繫目的，同時，Vigor 路由器可藉由真實 IP 位址與其他的網路裝置溝通連接。當資料經過時，路由器的網路位址轉換(NAT)功能將會在真實與虛擬位址間執行轉換動作，封包將可傳送至本地網路中正確的主機電腦上，如此一來，所有的主機電腦就都可以共享一個共同的網際網路連線。

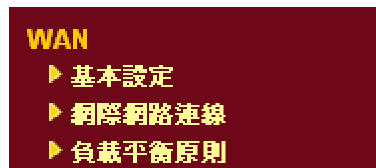
取得 ISP 提供的真實 IP 位址

欲取得 ISP 提供的真實 IP 位址，以便將路由器當成用戶假定之設備，有幾種種常見的模式可以選用：**Point to Point Protocol over Ethernet (PPPoE),** 和 **MPoA**.等，**Multi-PVC** 是提供給您執行更進階的設定。

在 ADSL 之部署中，PPP (Point to Point)型態之驗證和授權是橋接用戶前端設備所需要的。PPPoE (Point to Point Protocol over Ethernet)透過一台存取裝置連接網路主機至遠端存取集中器，此種應用讓使用者覺得操作路由器是很簡單的，同時也可依照使用者的需要提供存取控制及服務類型。

當路由器開始連接至 ISP 時，路由器將執行一系列過程以尋求連線，然後即可產生一個 session，您的使用者辨識名稱和密碼由 **RADIUS** 驗證系統的 **PAP** 或 **CHAP** 來驗證，通常您的 IP 位址、DNS 伺服器和其他相關資訊都是由 ISP 指派的。

下圖為 WAN 的功能項目：



3.1.2 基本設定

本節介紹數種網際網路的一般設定，並詳細說明 WAN1 和 WAN2 介面。

路由器支援雙 WAN 口功能，可讓使用者存取網際網路並整合雙 WAN 口的頻寬以加速網路資料傳輸。每個 WAN 連接埠(WAN1-透過 WAN 連結埠/WAN2-透過 LAN1 連接埠)可以連接到不同的 ISP，即使 ISP 使用不同的技術提供不同的電信服務(如 DSL, Cable 數據機等等)也都沒有問題。如果任何一個 ISP 連線出了問題，全部的傳輸動作都將引導並切換至正常的 WAN 口連接埠並繼續運行。

網頁允許您個別設定 WAN1 和 WAN2 的一般設定。

> **注意:** WAN1 預設狀態是啓動的，而 WAN2 則是視情況選擇的項目。

WAN >> 基本設定

基本設定

WAN1		WAN2	
啟用:	是	啟用:	是
顯示名稱:		顯示名稱:	
實體模式:	乙太網路	實體模式:	乙太網路
連線模式:	自動偵測	連線模式:	自動偵測
負載平衡模式:	自動權重	負載平衡模式:	自動權重
連線速度(Kbps):	下傳連線 0	連線速度(Kbps):	下傳連線 0
	上傳連線 0		上傳連線 0
啟動模式:	永遠連線	啟動模式:	永遠連線
需求時連線:		需求時連線:	
WAN2 連線失敗		WAN1 連線失敗	
WAN2 上傳速度超過 0 Kbps		WAN1 上傳速度超過 0 Kbps	
WAN2 下傳速度超過 0 Kbps		WAN1 下傳速度超過 0 Kbps	

確定

啓用	選擇是啓動此 WAN 界面的設定，選擇否則關閉此介面的設定。
顯示名稱	輸入 WAN1/WAN2 的說明內容。
實體模式	對 WAN1 而言，實體連線是透過 ADSL 連接埠來完成，不過 WAN2 的實體連接則是透過乙太網路連接埠來設定，這點是無法改變的。

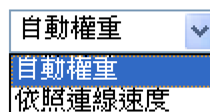
連線模式

您可以改變 WAN2 的連線模式，或是選擇**自動偵測**讓系統自行處理。



負載平衡模式

如果您知道 WAN 介面的實際頻寬，請選擇**依照連線速度**。否則請選擇**自動權重**，讓路由器來完成最佳的平衡結果。

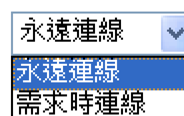


連線速度

如果您選擇**依照連線速度**作為負載平衡模式，請您輸入連線速度以便透過 WAN1/WAN2 介面上傳下載資料。單位是 kbps。

啓動模式

選擇**永遠連線**讓 WAN 連接(WAN1/WAN2)能永遠啓動運作；或是選擇**需求時連線**，讓 WAN 連接在有需要時才連上線。



如果您選擇的是需求時連線，即可為 PPPoE 和 PPTP 存取模式設定閒置逾時之時間，此外有三種選項供不同目的之需要來設定。

WAN2 連線失敗 – 表示 WAN1 在 WAN2 失敗時即自動連線。

WAN2 上傳速度超過 XX kbps – 表示當 WAN2 上傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN2 下傳速度超過 XX kbps – 表示當 WAN2 下載傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN1 連線失敗– 表示 WAN2 在 WAN1 失敗時即自動連線。

WAN1 上傳速度超過 XX kbps – 表示當 WAN1 上傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

WAN1 下傳速度超過 XX kbps – 表示當 WAN1 下載傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

3.1.3 網際網路連線控制

因為路由器支援雙 WAN 口功能，使用者得以設定不同的 WAN 設定供網際網路存取之用，又因為 WAN1 與 WAN2 的實體連線並不同，二者的連線模式也會有些差異。

WAN >> 網際網路連線

網際網路連線

索引編號	顯示名稱	實體模式	連線模式
WAN1		乙太網路	固定或動態 IP 細節設定
WAN2		乙太網路	無 細節設定

索引編號　　顯示路由器支援的 WAN 模式介面數，WAN1 是預設的 WAN 介面，WAN2 為 WAN1 無法運作時的選項介面。

顯示名稱　　顯示 WAN1/WAN2 於一般設定中所輸入的名稱。

實體模式　　顯示 WAN1/WAN2 的實體模式。

連線模式　　使用下拉式清單選擇適當的連線模式，接著按右邊的**細節設定**以設定詳細內容。

連線模式

固定或動態 IP
無
PPPoE
固定或動態 IP
PPTP

網頁提供三種連線模式 PPPoE, Static 或 Dynamic IP and PPTP。

細節設定　　此按鈕將依照您在 WAN1 或 WAN2 所選擇的連線模式展現不同的網頁內容。

PPPoE 細節設定

如果想要使用 PPPoE 作爲網際網路連線的通訊協定，請自 **WAN** 功能項目中選擇**網際網路連線**，接著在 WAN1 中選擇 PPPoE 模式，下面的細節設定網頁將會出現。

WAN >> 網際網路連線

WAN 1

PPPoE 用戶端模式

⦿ 啟用 ○ 停用

ISP 存取設定

使用者名稱 admin

密碼 ●●●●

索引號碼(1-15) 於 排程 設定:

=> , , ,

PPP/MP 設定

PPP 驗證 PAP 或 CHAP

閒置逾時 -1 秒

IP 位址指派方式 (IPCP) WAN IP別名

固定 IP: ○ 是 ⦿ 否 (動態IP)

固定 IP 位址

⦿ 預設 MAC 位址

○ 指定 MAC 位址

MAC 位址:

00 . 50 . 7F : C0 . 2F . F5

確定 取消

PPPoE 用戶端模式

按下**啓用**按鈕可啓動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。

ISP 存取設定

輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。

使用者名稱 –在本區請輸入 ISP 提供的使用者名稱。

密碼 – 在本區請輸入 ISP 提供的密碼。

索引號碼(1-15) 於排程設定 -可以輸入四組時間排程，全部的排程都是在**其他應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

PPP/MP 設定

PPP 驗證 – 選擇 **PAP** 或是 **PAP 或 CHAP**。

閒置逾時 – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間，此項設定只在 **WAN>>一般設定**網頁中的**啓動模式**選擇了**需求時連線**才會有作用。

IP 位址指派方式 (IPCP)

通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

WAN IP 別名 - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。

http://192.168.1.1 - WAN IP 別名 - Microsoft Internet Explorer

WAN IP 別名 (多重NAT)

索引編號	啟用	輔助 WAN IP	加入 NAT IP 配置群
1.	v	172.16.3.229	v
2.			
3.			
4.			
5.			
6.			
7.			
8.			

確定 全部清除 關閉

完成 網際網路

固定 IP 位址 – 按是以使用固定 IP 功能並輸入一個固定 IP 位址。

預設 MAC 位址 – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。

指定 MAC 位址 – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

固定或動態 IP 細節設定

對固定 IP 模式來說，通常您會收到 DSL 或是 ISP 服務供應商提供給您的一個固定的真實 IP 位址或是真實子網路，在大多數的情形下，Cable 服務供應商將會提供一個固定的真實 IP，而 DSL 服務供應商提供的是真實子網路資料。如果您有一組真實的子網路，您可以指派一組或是多組 IP 位址至 WAN 介面。

若要使用**固定或動態 IP** 為網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線**，接著選擇**固定或動態 IP**，即可出現下圖。

WAN >> 網際網路連線

WAN 1

固定或動態 IP（DHCP用戶端）
⦿啟用 ○停用

維持 WAN 連線
☐ 啟用 PING 以保持常態連線
PING 到指定的 IP 位址
PING 間隔 0 分

RIP 協定
☐啟用 RIP

WAN IP 網路設定 [WAN IP 別名]
○ 自動取得 IP 位址
路由器名稱 *
網域名稱 *
* : 有些 ISP 需要此項設定名稱
⦿ 指定 IP 位址
IP 位址 172.16.3.229
子網路遮罩 255.255.0.0
閘道 IP 位址 172.16.3.4

⦿ 預設 MAC 位址
○ 指定 MAC 位址
MAC 位址:
00 . 50 . 7F : C0 . 2F . F5

DNS 伺服器 IP 位址
主要 IP 位址
次要 IP 位址

[確定] [取消]

固定或動態 IP (DHCP 用戶端)	按啟用以啟動此功能，如果您按的是停用，此功能將會關閉，您在此頁面所完成的全部設定都將失效。
維持 WAN 連線	正常情況下，這個功能是設計用來符合動態 IP 環境，因為某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啟用 PING 以保持常態連線**。 **PING 到指定的 IP** – 如果您啟用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線 **PING 間隔** - 輸入間隔時間讓系統得以執行 PING 動作。
RIP 協定	Routing Information Protocol 縮寫為 RIP(RFC1058)，指名路由器是如何變更路由表格資訊，勾選此項目以啟動此功能。
WAN IP 網路設定	這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。 **WAN IP 別名** - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對

WAN1 有效用。

http://192.168.1.1 - WAN IP 別名 - Microsoft Internet Explorer

WAN IP 別名 (多重NAT)

索引編號	啟用	輔助 WAN IP	加入 NAT IP 配置群
1.	v	172.16.3.229	v
2.	☐		☐
3.	☐		☐
4.	☐		☐
5.	☐		☐
6.	☐		☐
7.	☐		☐
8.	☐		☐

確定 全部清除 關閉

完成 網際網路

自動取得 IP 位址 – 如果您想要使用**動態 IP** 模式,按此鈕以自動取得 IP 位址。

路由器名稱: 輸入 ISP 的路由器名稱。

網域名稱: 輸入指定的網域名稱。

指定 **IP** 位址 – 按此鈕指定 IP 位址讓資料通過。

IP 位址:輸入 IP 位址。

子網路遮罩:輸入子網路遮罩。

*閘道 **IP** 位址*: 輸入閘道 IP 位址。

*預設 **MAC** 位址*: 按此鈕使用預設的 MAC 位址。

*指定 **MAC** 位址*: 部分 Cable 服務供應商會指定 MAC 位址作爲存取驗證之用,此時您需要按下此鈕並在下方區域輸入 MAC 位址。

DNS 伺服器 IP 位址 若要使用固定 IP 模式,請輸入路由器的**主要 IP 位址**,如有必要,在將來,您也可以輸入**次要 IP 位址**以符合所需。

PPTP 細節設定

若要使用 **PPTP** 爲網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線**，接著選擇 **PPTP**，即可出現下圖。

WAN >> 網際網路連線

WAN 1

PPTP 用戶端模式

啟用 停用

PPTP 伺服器 10.0.0.138

ISP 存取設定

使用者名稱

密碼

索引號碼(1-15) 於 排程 設定:

=> , , ,

ISDN 撥接備援設定

撥接備援模式 無

PPP 設定

PPP 驗證 PAP或 CHAP

閒置逾時 -1 秒

IP 位址指派方式 (IPCP) WAN IP 別名

固定 IP: 是 否 (動態IP

固定 IP 位址

WAN IP 網路設定

自動取得 IP 位址

指定 IP 位址

IP 位址 10.0.0.150

子網路遮罩 255.0.0.0

確定 取消

PPTP 設定	**PPTP 連結** -勾選啓用讓 PPTP 用戶得以在廣域網路介面上建立連接到 DSL 數據機的通道。
ISP 存取設定	**使用者名稱** - 輸入 ISP 業者提供給您的使用者名稱。 **密碼** - 輸入 ISP 業者提供的密碼。 **索引號碼 (1-15) 於排程設定** - 您可以輸入四組時間排程設定，所有的排程都是在時間**排程設定**網頁中事先設定完畢，您可直接輸入該時間排程的號碼即可。
PPP 設定	**PPP 驗證** – 選擇 **PAP** 或是 **PAP** 或 **CHAP**。 **閒置逾時** - 閒置逾時表示路由器在一段時間內都沒有運作時，就會中斷連線。這項設定只有您在 WAN 的**一般設定**中選取了**永遠連線**時才會有效。
IP 位址指派方式 **(IPCP)**	**WAN IP** 別名 - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。

http://192.168.1.1 - WAN IP 別名 - Microsoft Internet Explorer

WAN IP 別名 (多重NAT)

索引編號	啟用	輔助 WAN IP	加入 NAT IP 配置群
1.	v	172.16.3.229	v
2.			
3.			
4.			
5.			
6.			
7.			
8.			

確定 全部清除 關閉

完成 網際網路

固定 IP - 通常每一次您要求連線時，ISP 會浮動指定 IP 位址給您使用，但在某些情況下，ISP 總是提供相同的 IP 位址予您，因此您可以在固定 IP 位址區域中輸入此 IP 位址，在您輸入並使用此項功能之前，請先聯絡您的 ISP 業者取得相關資訊，再選擇**是**並輸入固定 IP 位址以便使用。

固定 IP 位址 – 請輸入固定 IP 位址。

WAN IP 網路設定

自動取得 IP 位址 – 按此鈕以自動取得 IP 位址。
指定 IP 位址 – 按此鈕以指定 IP 位址。
IP 位址 – 輸入 IP 位址。
子網路遮罩 – 輸入子網路遮罩。

3.1.4 負載平衡原則

路由器支援負載平衡功能，可以將通訊協定之類型、指定主機的 IP 位址、主機子網路以及通訊埠範圍指派至 WAN1 或是 WAN2 介面。使用者可以指定流量的類型並基於此網頁之設定，強迫封包前往特定網路介面。本路由器支援 20 組的原則。

注意:負載平衡原則只在 WAN1 和 WAN2 都啓動的情形下才能執行。

WAN >> 負載平衡原則

負載平衡原則

索引編號	啟用	通訊協定	WAN	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標通訊埠起點	目標通訊埠終點
1	☐	任意							
2	☐	任意							
3	☐	任意							
4	☐	任意							
5	☐	任意							
6	☐	任意							
7	☐	任意							
8	☐	任意							
9	☐	任意							
10	☐	任意							

<< 1-10 | 11-20 >> 下一頁 >>

索引編號　　按下任何一個索引號碼以進入負載平衡原則設定頁面。

啓用　　勾選此方塊以啓用此原則。

通訊協定　　使用下拉式功能以變更 WAN 介面的通訊協定。

任意
TCP
UDP
TCP/UDP
ICMP
IGMP

WAN　　使用下拉式功能以變更 WAN 介面。

WAN1
WAN2

來源 **IP** 起點　　顯示來源 IP 起點的 IP 位址。

來源 **IP** 終點　　顯示來源 IP 終點的 IP 位址。

目標 **IP** 起點　　顯示目標 IP 起點的 IP 位址。

目標 **IP** 終點　　顯示目標 IP 終點的 IP 位址。

目標通訊埠起點　　顯示目標通訊埠起點的埠號。

目標通訊埠終點　　　　顯示目標通訊埠終點的埠號。

按索引編號 **1** 進入下述頁面設定負載平衡原則。

WAN >> 負載平衡原則

索引編號: 1

☐ 啟用	
通訊協定	TCP
綁定 WAN 介面	WAN1
來源 IP 起點	192.168.1.3
來源 IP 終點	192.168.1.5
目標 IP 起點	168.95.0.0
目標 IP 終點	168.95.0.100
目標通訊埠起點	80
目標通訊埠終點	100

確定　取消

啓用　　　　勾選此方塊以啓動此原則。

通訊協定　　　　使用下拉式選項選擇 WAN 介面適合的通訊協定。

通訊協定　TCP
- 任何一種
- TCP
- UDP
- TCP/UDP
- ICMP
- IGMP

綁定 WAN 介面　　　　選擇一個 WAN 介面(WAN1 或 WAN2)作爲綁定介面。

來源 **IP** 起點　　　　輸入指定 WAN 介面的來源 IP 起點位址。

來源 **IP** 終點　　　　輸入指定 WAN 介面的來源 IP 終點位址。 如果本區空白，即表示區域網路中全部的來源 IP 位址都可由此 WAN 介面通過。

目標 **IP** 起點　　　　輸入指定 WAN 介面的目標 IP 起點位址。

目標 **IP** 終點　　　　輸入指定 WAN 介面的目標 IP 終點位址。如果本區空白，即表示區域網路中全部的目標 IP 位址都可由此 WAN 介面通過。

目標通訊埠起點　　　　輸入目標通訊埠的起點埠號。

目標通訊埠終點　　　　輸入目標通訊埠的終點埠號。如果本區空白，即表示區域網路中全部的目標通訊埠都可由此 WAN 介面通過。

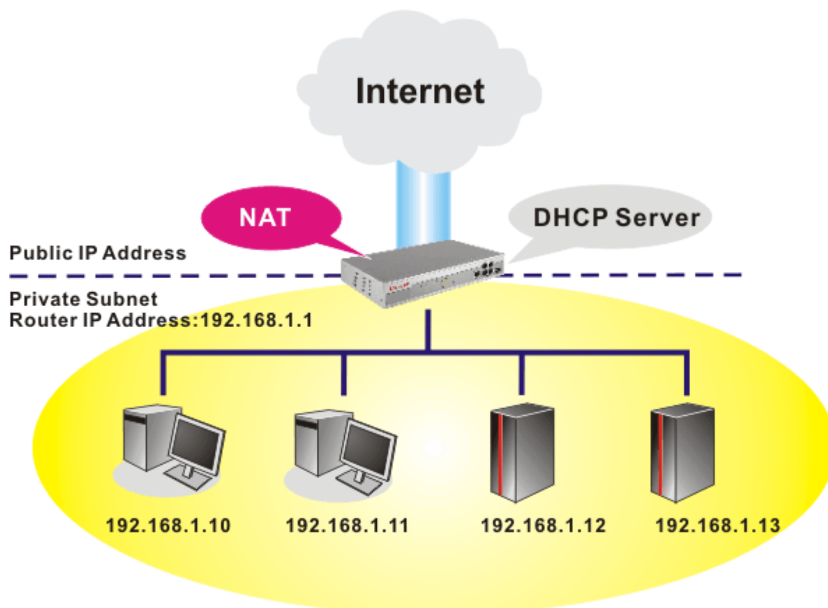
3.2 區域網路(LAN)

區域網路是由路由器所管理的一群子網路，網路結構設計和您自 ISP 所取得之真實 IP 位址有關。

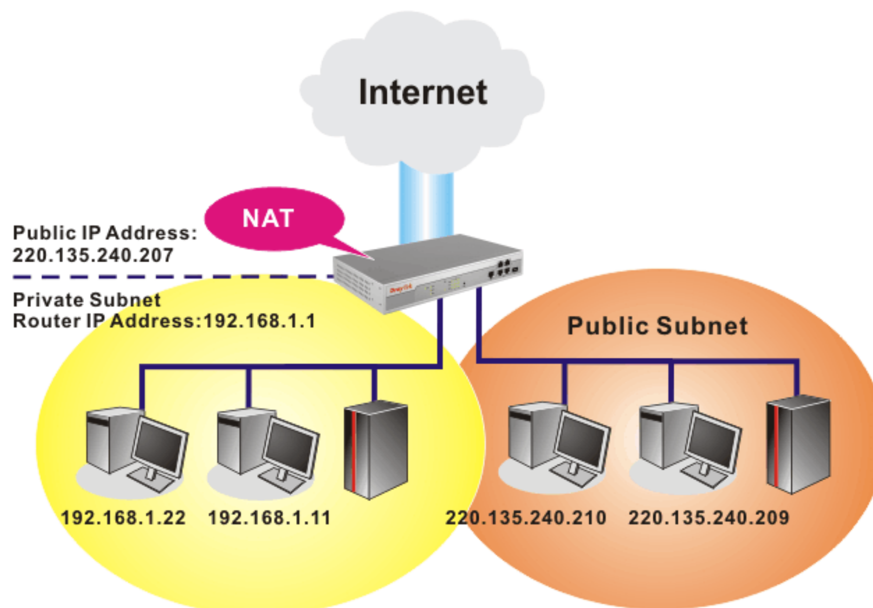


3.2.1 區域網路基本概念

Vigor 路由器最基本的功能為 NAT，可用來建立虛擬的子網路，如前所述，路由器利用真實 IP 位址與網際網路上其他的真實主機互相通訊，或是使用虛擬 IP 地址與區域網路上的主機連繫。NAT 要完成的事情就是轉換來自真實 IP 位址的封包到私有 IP 地址，以便將正確的封包傳送至正確的主機上，反之亦然。此外 Vigor 路由器還有內建的 DHCP 伺服器，可指定虛擬 IP 地址至每個區域主機上，請參考下面的範例圖，即可獲得大略的了解。



在某些特殊的情形當中，您可能會有 ISP 提供給您的真實 IP 子網路像是 220.135.240.0/24，這表示您可以設定一個真實子網路，或是使用配備有真實 IP地址之主機的第二組子網路，作為真實子網路的一部份，Vigor 路由器將會提供 IP 路由服務，幫助真實地區子網路上的主機能與其他真實主機/外部伺服器溝通連繫，因此路由器必須設定為真實主機的通訊閘道才行。



什麼是 RIP(Routing Information Protocol)

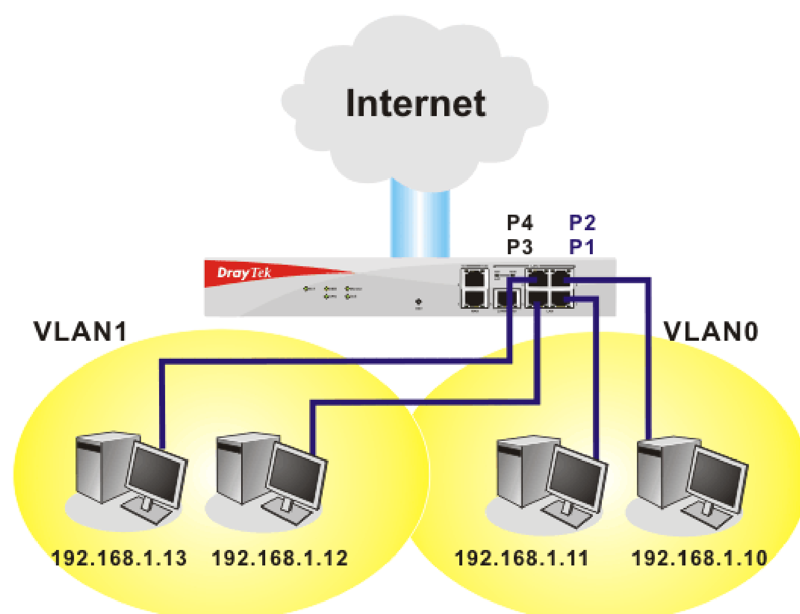
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

什麼是固定路由

當您的區域網路上有數個子網路時，比起其他的方法有時候對連線來說最有效也是最快速的方式就是固定路由功能，您可設定一些規則來傳送指定子網路上的資料到另一個指定的子網路上而不需要透過 RIP。

什麼是虛擬區域網路(VLAN)

您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。為了要管理不同群組間的通訊狀況，請再虛擬區域網路功能上設定一些規則，以及每個網路的傳送速率。



3.2.2 基本設定

本頁提供您區域網路的基本設定。

按**區域網路**開啓區域網路設定並選擇**基本設定**。

區域網路 >> 基本設定

區域網路 TCP / IP與 DHCP 設定

區域網路 IP 網路組態		DHCP 伺服器組態	
供 NAT 使用		⦿啟用 ○停用	
第一 IP 位址	192.168.1.1	DHCP 中繼代理位址 ○第一子網路 ○第二子網路	
第一子網路遮罩	255.255.255.0	起始 IP 位址	192.168.1.10
供 IP 路由使用 ○ 啟用 ⦿ 停用		IP 配置數量	50
第二 IP 位址	192.168.2.1	閘道 IP 位址	192.168.1.1
第二子網路遮罩	255.255.255.0	中繼代理程式IP位址	
	第二子網路 DHCP 伺服器	DNS 伺服器 IP 位址	
		☐ 使用 DNS 手動設定	
RIP 協定控制	停用	主要 IP 位址	
		次要 IP 位址	

確定

第一 IP 位址	請輸入虛擬 IP 地址以便連接區域虛擬網路(預設值爲 192.168.1.1)。
第一子網路遮罩	請輸入決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。
供 IP 路由使用	按下**啓用**以啓動此功能，此功能預設值是**停用**。此應用視情況需要而設定。
第二 IP 位址	請輸入第二組 IP 地址以便連接至子網路(預設值爲 192.168.2.1)。
第二子網路遮罩	請輸入第二組決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。
第二子網路遮罩 DHCP 伺服器	您可以將路由器設定爲 DHCP 伺服器，提供服務予第二組子網路。



起始 IP 位址：輸入 IP 地址 pool 數值做為 DHCP 伺服器指定 IP 地址時的起始點，如果路由器的第二組 IP 地址為 220.135.240.1,，起始 IP 地址可以是 220.135.240.2 或是更高一些，但比 220.135.240.254 小。

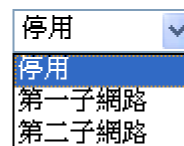
IP 配置數量：輸入 IP 地址的數量，最大值為 10，例如您若輸入 3 而第二組 IP 地址為 220.135.240.1，DHCP 伺服器的 IP 地址範圍即為 220.135.240.2 到 220.135.240.4。

MAC 位址：請一個個輸入主機的 MAC 地址，按**新增**來建立主機清單以便指定、刪除或是編輯上述範圍中的 IP 地址。設定第二組 DHCP 伺服器所需的 MAC 位址清單，可幫助路由器指定正確的 IP 地址及子網路至正確的主機上。這樣在第二子網路上的主機便不會得到屬於第一組子網路的 IP 地址。

RIP 協定控制

停用 – 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此為預設值)。

RIP 協定控制



第一子網路-選擇路由器以交換第一子網路和鄰近路由器間的 RIP 資訊。

第二子網路-選擇路由器以交換第二子網路和鄰近路由器間的 RIP 資訊。

DHCP 伺服器組態

DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作為您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成為 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。

如果您想要使用網路上另外的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。

啓用 - 讓路由器指定 IP 地址到區域網路上的每個主機上。

停用 – 讓您手動指定 IP 地址到區域網路上的每個主機上。

DHCP 中繼代理位址 - **(**第一子網路/第二子網路**)** 指定某個 DHCP 伺服器所在的子網路讓中繼代理重新引導 DHCP 需求至該處。

起始 IP 位址 -輸入 DHCP 伺服器的 IP 地址配置的數值作爲指定 IP 地址的起始點，如果第路由器的第一個 IP 地址爲 192.168.1.1，起始 IP 地址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。

IP 配置數量 -輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 50，最大值爲 253。

閘道 IP 位址 -輸入 DHCP 伺服器所需的閘道 IP 地址，這項數值通常與路由器的第一組 IP 地址相同，表示路由器爲預設的閘道。

中繼代理程式 IP 位址 -設定您預備使用的 DHCP 伺服器 IP 位址，讓中繼代理可以協助傳送 DHCP 需求至伺服器上。

DNS 伺服器組態

DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 地址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。

使用 DNS 手動設定 – 強迫路由器使用本頁所指定的 DNS 伺服器而非使用網際網路存取伺服器所提供的 DNS 伺服器 (PPPoE, PPTP, L2TP 或 DHCP 伺服器).

主要 IP 位址 -您必須在此指定 DNS 伺服器的 IP 地址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。

次要 IP 位址 - 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址爲 194.98.0.1，放在此區域。

預設 DNS 伺服器 IP 位址可在線上狀態上查看:

連線狀態 已開機時間: 16:7:58

區域網路狀態 主要 DNS: 194.109.6.66 次要 DNS: 168.95.1.1

IP 位址	傳送封包	接收封包
192.168.1.1	12778	7441

如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 地址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。

如果網域名稱的 IP 地址已經在 DNS 快速緩衝貯存區內，路由器將立即 resolve 網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

第五章中舉出常見的區域網路設定腳本供您參考，有關設定範例部份，如有需求請參考該章以取得更多的訊息。

3.2.3 固定路由

進入**區域網路**群組並選擇**固定路由**，開啓如下的畫面。

區域網路 >> 固定路由設定

固定路由組態 | **回復出廠預設值** | **檢視路由表** |

索引編號	目標位址	狀態	索引編號	目標位址	狀態
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

狀態: v 一 使用中，x 一 未使用，? 一 空白

索引編號	索引編號下方的號碼(1 到 10)允許您開啓下一層頁面以設定固定路由。
目標位址	顯示固定路由的目標位址。
狀態	顯示固定路由的狀態。
檢視路由表	開啓如下畫面檢視目前的路由狀況。

自我診斷工具 >> 檢視路由表

目前執行中的路由表 | **更新頁面** |

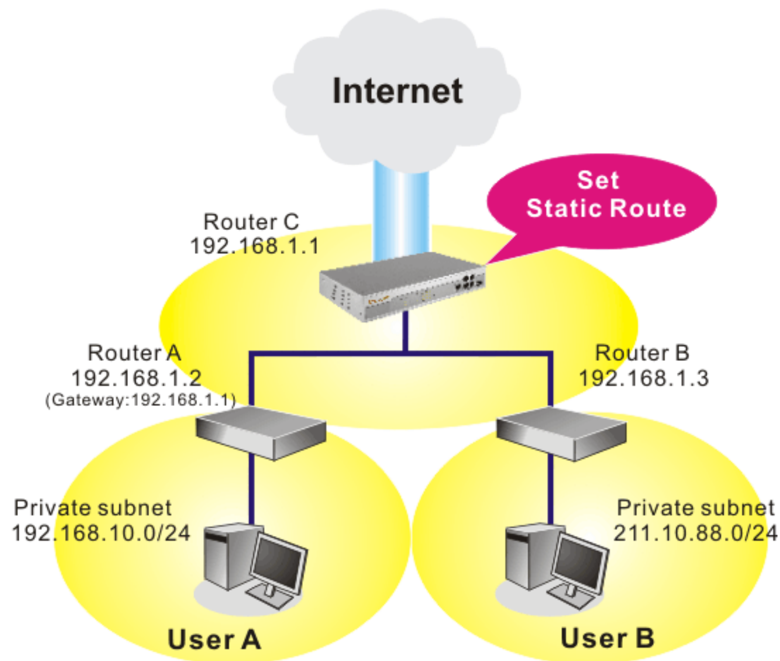
```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*          0.0.0.0/         0.0.0.0 via 172.16.3.4,   WAN1
C~       192.168.1.0/   255.255.255.0 is directly connected,    LAN
C         172.16.0.0/     255.255.0.0 is directly connected,   WAN1
```

增加固定路由至虛擬或真實網路上

此處爲固定路由的範例，不同子網路上的使用者 A 與 B 可以透過路由器彼此溝通。假定網際網路的存取已設定完畢，路由器可以適當的運作。

- 使用主要路由器進入網際網路
- 利用內部的路由器 A(192.168.1.2)，建立虛擬子網路 192.168.10.0
- 透過內部的路由器 B(192.168.1.3)，建立真實子網路 211.100.88.0
- 已設定主要路由器 192.168.1.1 爲路由器 A (192.168.1.2) 的預設閘道

在設定固定路由之前，使用者 A 無法與使用者 B 溝通，因爲路由器 A 只會傳送辨認出的封包至主要路由器的預設閘道。



1. 在**區域網路**群組中，選擇**一般設定**。再選擇第一子網路作為 **RIP 協定控制**，然後點選**確定**按鈕。

   > 注意：有二個理由讓我們一定要在第一子網路上應用 RIP 通訊協定。第一個理由是區域網路介面可以透過第一子網路(192.168.1.0/24)與鄰近路由器作 RIP 封包交換，第二個，理由是網際網路虛擬子網路上(例如 192.168.10.0/24)的主機群可以藉此路由器存取網際網路資訊，並和不同子網路持續進行 IP 路由資訊交換。

2. 在**區域網路**群組中，選擇固定路由，按索引編號 1 勾選**啟用**方塊， 請以下列數字新增一個固定路由，讓所有應前往 192.168.10.0 的封包都能透過 192.168.1.2 來轉送，接著按**確定**。

區域網路 >> 固定路由設定

索引編號 1

☑ 啟用

目的 IP 位址	192.168.10.0
子網路遮罩	255.255.255.0
閘道 IP 位址	192.168.1.2
網路介面	LAN

確定　取消

3. 回到**固定路由**頁面，按另一個索引編號增加另一個固定路由，設定如下圖。它可將所有指定前往 211.100.88.0 的封包轉送至 192.168.1.3，然後按**確定**。

區域網路 >> 固定路由設定

索引編號 1

☑ 啟用

目的 IP 位址	211.100.88.0
子網路遮罩	255.255.255.0
閘道 IP 位址	192.168.1.3
網路介面	LAN

確定 取消

4. 按**自我診斷工具**中的**路由表**檢查目前的路由表格。

自我診斷工具 >> 檢視路由表

目前執行中的路由表 | 更新頁面 |

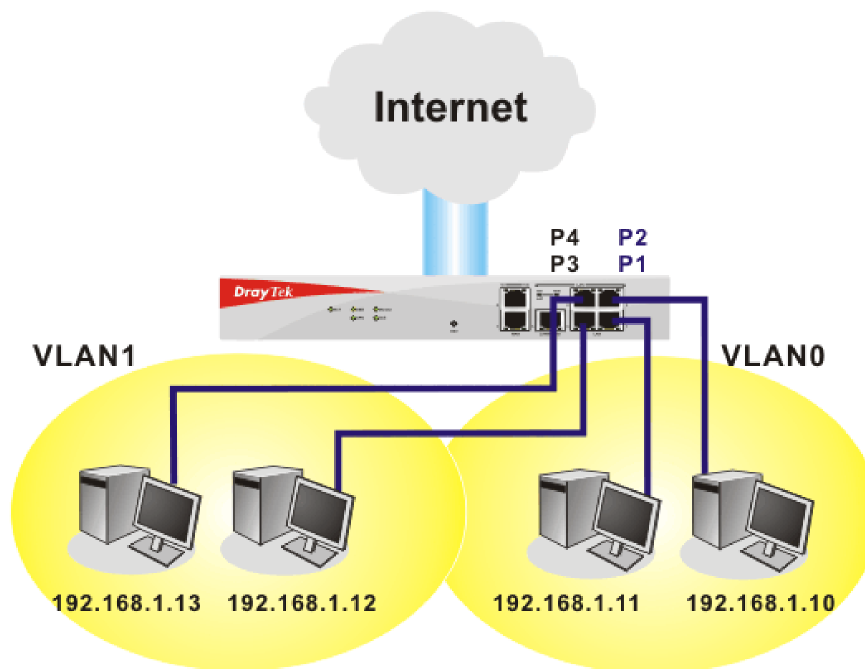
```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*           0.0.0.0/          0.0.0.0 via 172.16.3.4,    WAN1
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2,    LAN
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
C          172.16.0.0/     255.255.0.0 is directly connected,    WAN1
```

3.2.4 VLAN (虛擬區域網路)

注意：此功能僅適用於 **Vigor2950** 機種，如果您是 Vigor2950G 的用戶，請參考 3.11 一節。

VLAN（虛擬區域網路）的功能提供您一個方便的方式，藉由群組實體通訊埠上的連結主機達到管理的目的。

連接上乙太網路連接埠的電腦可以區分成不同的群組且形成虛擬區域網路，在相同群組下的電腦可以透過路由器共享彼此的資訊，且不會受到其他群組的影響。



您可透過有線連接的方式，來設定虛擬區域網路設定以達成上述的目的。只要簡單的勾選 VLAN0 該行的 P1 和 P2 方塊，以及 VLAN1 該行的 P3 和 P4 方塊即可。

區域網路 >> VLAN 設定

VLAN 設定

☑啟用

	P1	P2	P3	P4
VLAN0	☑	☑	☐	☐
VLAN1	☐	☐	☑	☑
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

[確定] [清除] [取消]

啓用	勾選此方塊啓用此功能。
P1 – P4	勾選方塊讓連結至連接埠上的電腦都可群組至指定的 VLAN。注意每個通訊埠都可同時在群組在不同的 VLAN，只要您勾選該相對方塊即可，例如您勾選了 VLAN0-P1 和 VLAN1-P1，您可以讓 P1 同時群組在 VLAN0 和 VLAN1 之下。
VLAN0-3	路由器允許您設定 4 組虛擬的區域網路。

3.2.5 綁定 IP 與 MAC 位址

此功能用來綁定區域網路中的電腦之 IP 與 MAC 位址，如此一來可在網路上達到更有效的控制。當此一功能啓用時，所有被綁定的 IP 與 MAC 位址的電腦都不能在變更，如果您修改了綁定 IP 或 MAC 位址，可能會造成無法存取網際網路的窘態。

按**區域網路**並選擇**綁定 IP 與 MAC 位址**開啓設定網頁。

區域網路 >> 綁定 IP 與 MAC 位址

綁定 IP 與 MAC 位址

附註: IP-MAC 綁定中事先調整之DHCP配置
如果選擇了限制綁定項目，任何一個未與MAC綁定的IP即無法存取網際網路。

◉ 啟用 ○ 停用 ○ 限制綁定

ARP 表 | 全選 | 排序 | 更新頁面 |

IP 位址	MAC 位址
192.168.1.10	00-0E-A6-2A-D5-A1
192.168.1.18	00-12-F0-11-2C-E4
192.168.1.100	00-08-A1-36-97-5D

IP 綁定清單 | 全選 | 排序 |

索引編號	IP 位址	MAC 位址

新增與編輯

IP 位址

MAC 位址

新增 編輯 刪除

確定

啓用	按此鈕啓用此功能，不過未列在 IP 綁定清單中的 IP/MAC 位址以可以連上網際網路。
停用	按此鈕關閉此功能，頁面上全部的設定都將會失效。
限制綁定	按此鈕封鎖未列在 IP 綁定清單中的 IP/MAC 位址連線。
ARP 表	此表格爲路由器的區域網路 ARP 表，IP 和 MAC 資訊將顯示於本區。列於 ARP 表中的每組 IP 和 MAC 位址都可以爲使用者挑選並透過**新增**按鈕加到 IP 綁定清單上。
全選	按此連結選擇表格內全部內容。
排序	按此連結將表格內容按照 IP 位址重新排序。
更新頁面	用來更新 ARP 表格，當新的電腦增加到區域網路上時，您可以按此連結取得最新的 ARP 表格資訊。
新增與編輯	**IP 位址** – 輸入 IP 位址以作爲指定 MAC 位址之用。 **MAC 位址** – 輸入 MAC 位址以便與指定的 IP 位址綁在一起。
IP 綁定清單	顯示綁定 IP 至 MAC 資訊清單。
新增	允許您將 ARP 表格中所挑選的或是在新增和編輯上所輸入的 IP/MAC 位址新增至 **IP 綁定清單**上。

編輯	允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。
刪除	您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單**上刪除。

附註: 在您選擇**限制綁定**前，您必須為一台電腦設定一組 IP/MAC 位址，若無設定的話，沒有一台電腦可以連上網際網路，路由器的網頁組態設定也無法進入了。

3.3 NAT

通常，路由器可以 NAT 路由器提供其相關服務，NAT 是一種機制，一個或多個虛擬 IP 位址可以對應到某個單一的真實 IP 位址。真實 IP 位址習慣上是由您的 ISP 所指定的，因此您必須為此負擔費用，虛擬 IP 位址則只能在內部主機內辨識出來。

當封包之目的地位址為網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成為真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

NAT 的好處如下：

- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

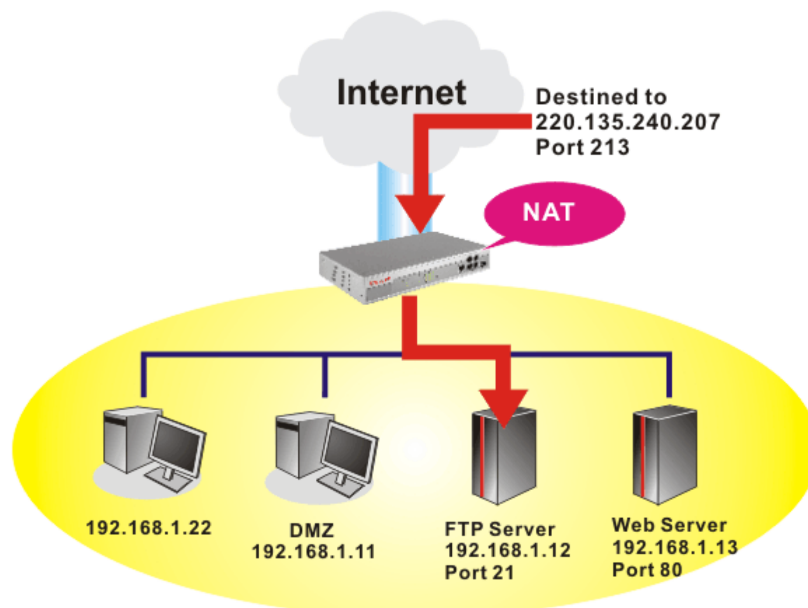
在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

下圖為 NAT 功能項目：



3.3.1 通訊埠重導向

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以爲所有使用者所辨識。既然此伺服器實際坐落於區域網路內，因此網路可以受到路由器之 NAT 的詳密保護，且可由虛擬 IP 位址/通訊埠來辨認。通訊埠重導向表的功能是傳送所有來自外部使用者對真實 IP 位址之存取需求，以對應至伺服器的虛 IP 位址/通訊埠。



通訊埠重導向只能應用在流入的資料量上。

欲使用此項功能，請開啓 **NAT** 頁面然後選擇**通訊埠重導向**。**通訊埠重導向**提供 10 組通訊埠對應入口給予內部主機對應使用。

NAT >> 設定通訊埠重導向表

通訊埠重導向表

#	模式	服務名稱	通訊協定	對外通訊埠	虛擬 IP	虛擬通訊埠	啟用
1	單一		---	0		0	☐
2	單一		---	0		0	☐
3	單一		---	0		0	☐
4	單一 範圍		---	0		0	☐
5	單一		---	0		0	☐
6	單一		---	0		0	☐
7	單一		---	0		0	☐
8	單一		---	0		0	☐
9	單一		---	0		0	☐
10	單一		---	0		0	☐

附註：在"範圍" 模式下，若IP位址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。

確定　清除

模式　　有二種模式可以供使用者選擇 - **單一**與**範圍**，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位址與第

一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。

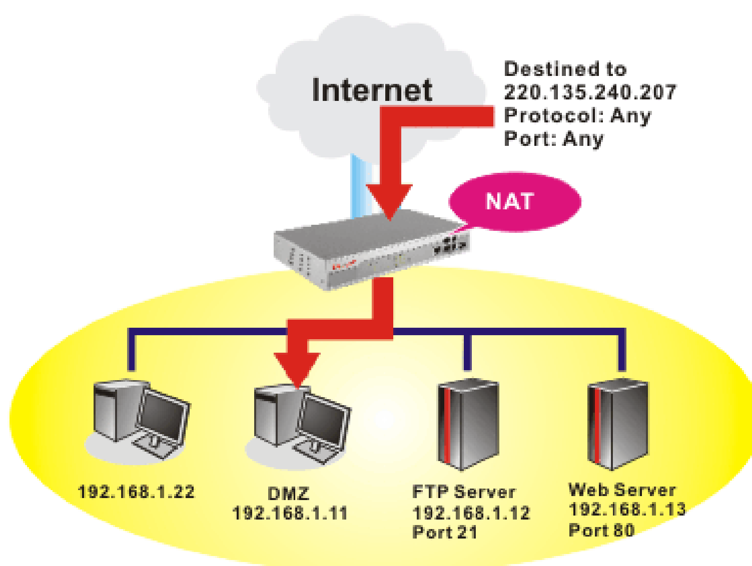
服務名稱	輸入特定網路服務的名稱。
通訊協定	選擇傳送層級的通訊協定(TCP 或 UDP)。
對外通訊埠	指定哪一個通訊埠可以重新導向至內部主機特定的虛擬 IP 通訊埠上。如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。
虛擬 IP	指定提供服務的主機之 IP 位址，如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。
虛擬通訊埠	指定內部主機提供服務之虛擬通訊埠號。
啓用	勾選此方塊以啓動您所定義的通訊埠對應功能。

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啓動路由器以避免衝突發生。

例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何一種都可以（例如 8080），來防止衝突發生。在**系統管理**群中的**管理設定**可以做此調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80)來進入管理畫面。

3.3.2 DMZ 主機設定

如同上面所提及的內容，通訊埠重導向可以將流入的 TCP/UDP 或是特定通訊埠中其他的流量，重新導向區域網路中特定主機之 IP 位址/通訊埠。不過其他的 IP 協定例如協定 50 (ESP)和 51(AH)是不會在固定通訊埠上行動的，Vigor 路由器提供一個很有效的工具 DMZ 主機，可以將任何協定上的需求資料對應到區域網路的單一主機上。來自用戶端的正常網頁搜尋和其他網際網路上的活動將可繼續進行，而不受到任何打擾。DMZ 主機允許內部被定義規範的使用者完全暴露在網際網路上，通常可促進某些特定應用程式如 Netmeeting 或是網路遊戲等等的進行。



注意：NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

請按 **DMZ 主機設定**開啓下述頁面：

NAT >> DMZ 主機設定

DMZ 主機設定

WAN 1

虛擬 IP

虛擬 IP 選擇電腦

真實IP DMZ主機的 MAC 00 : 00 : 00 : 00 : 00 : 00

附註：當啟用真實 IP 的 DMZ 主機時，WAN 會永遠保持連線。

WAN 2

開啟 虛擬 IP 選擇電腦

確定

WAN1 本頁允許您設定虛擬 IP 或是啓用真實 IP 位址作爲 DMZ 主機之用。

虛擬 IP 如果您在 WAN1 選項中選擇虛擬 IP 作爲 DMZ 主機，請在此輸入虛擬 IP 位址或是按選擇電腦按鈕挑選一個位址。

真實 IP DMZ 主機的 若您選擇啓用真實 IP 作爲 DMZ 主機位址，請在此區域輸入

MAC 位址 該主機的 MAC 位址。

如果您在**網際網路連線設定**選擇 **PPPoE**，並且設定 **WAN 別名**，您將可在此頁面發現**輔助 WAN IP** 項目。

NAT >> DMZ 主機設定

DMZ 主機設定

WAN 1

索引	開啟	輔助 WAN IP	虛擬 IP	
1.	☑	192.168.1.99		選擇電腦

WAN 2

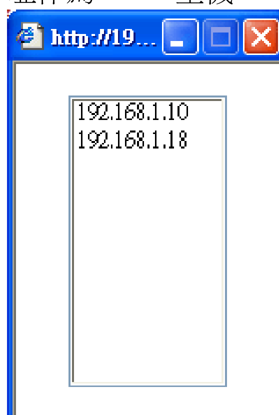
開啟	虛擬 IP	
☐		選擇電腦

確定 清除

開啓 勾選此項以啓動 DMZ 主機功能。

虛擬 IP 輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 PC** 開啓另一頁面來選擇。

選擇電腦 按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作為 DMZ 主機。



當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。

NAT >> DMZ 主機設定

DMZ 主機設定

WAN 1

索引	開啟	輔助 WAN IP	虛擬 IP	
1.	☑	192.168.1.99	192.168.1.10	選擇電腦

WAN 2

開啟	虛擬 IP	
☐		選擇電腦

確定 清除

3.3.3 開放通訊埠

開放通訊埠允許您開啓一段範圍內的通訊埠，供特定應用程式使用。常見的應用程式包含有 P2P 應用程式(如 BT、KaZaA、Gnutella、WinMX、eMule 和其他)、Internet Camera 等等，您需要先確定應用程式包含最新的資料，以免成爲安全事件的受害者。

按**開放通訊埠**連結開啓下面的網頁。

NAT >> 開放通訊埠

開放通訊埠設定 | 回復出廠預設值 |

索引編號	註解	WAN 介面	內部 IP 位址	狀態
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >> 下一頁 >>

索引編號	表示本地主機中您想要提供之服務，其特定內容網頁之相關號碼，您應該選擇適當的索引號碼以編輯或是清除相關的內容。
註解	指定特定網路服務的名稱。
WAN 介面	顯示該項設定之 WAN 介面。
內部 **IP** 位址	顯示提供此項服務之本地主機的 IP 位址。
狀態	顯示每項設定的狀態，X 或 V 表示關閉或是啓用狀態。

如果要新增或是編輯通訊埠設定，請按索引下方的號碼按鈕。該索引號碼入口設定頁面隨即出現，在每個輸入頁面中，您可以指定 10 組通訊埠範圍給予不同的服務。

NAT >> 開放通訊埠 >> 編輯開放通訊埠

索引編號 1

☑ 啟用開放通訊埠

說明

WAN 介面 WAN1

WAN IP 192.168.1.99

本機電腦 192.168.1.10 選擇電腦

	通訊協定	起始通訊埠	結束通訊埠		通訊協定	起始通訊埠	結束通訊埠
1.	TCP	4500	4700	6.	-----	0	0
2.	UDP	4500	4700	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

確定 清除 取消

啓用開放通訊埠	勾選此項以啓動此功能。
說明	請爲所定義的網路應用/服務命名。
WAN 介面	指定該項設定之 WAN 介面。
WAN IP	如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現 **WAN IP** 項目。請自下拉式選項中選擇需要的 IP 位址。
本機電腦	輸入本機的虛擬 IP 位址或是按**選擇電腦**挑選另外一個。
選擇電腦	按此鈕後另一個視窗即自動跳出並提供本機的虛擬 IP 位址之清單資料，請自清單中選取最適宜的 IP 位址。
通訊協定	指定傳送層級的通訊協定，有 **TCP**、**UDP** 和 **----- (none)**等幾種選擇。
起始通訊埠	指定本機所提供之服務的開始通訊埠號。
結束通訊埠	指定本機所提供之服務的結束通訊埠號。

3.4 物件設定

對某些範圍內的 IP 和侷限於特定區域的服務通訊埠，通常可以套用於路由器網頁設定中。因此我們可以將他們定義成為物件，並結合成群組以便後續能方便的應用。之後，我們可以選擇該物件/群組來套用，比方說，相同部門內所有的 IP 可定義成為一個 IP 物件(意即 IP 位址範圍)。



3.4.1 IP 物件

您可設定 192 組不同條件的 IP 物件。

物件設定 >> IP 物件

IP物件設定檔: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> 下一頁 >>

回復出廠預設值	清除全部的設定資料。

按下任一索引號碼進入下述畫面：

物件設定 >> IP 物件

設定檔索引 : 1

名稱:	RD部門
介面:	任何一種
位址類型:	位址範圍
起始 IP 位址:	192.168.1.64
結束 IP 位址:	192.168.1.75
子網路遮罩:	0.0.0.0
反向選擇:	☐

確定 取消

名稱	請輸入本設定檔的名稱，最多可以輸入 15 個字元。例如 RD 部門或研發部門等等。
介面	請選擇適當的介面(WAN, LAN 或是任何一種)。 介面 任何一種 任何一種 LAN WAN 例如，**編輯過濾器規則**中的**方向**設定會要求您針對 WAN 或 LAN 介面指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN 作爲介面，並選擇 LAN 作爲**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。
位址類型	決定 IP 位址的位址類型。 如果物件僅包含 IP 位址的話，請選擇**單一位址**。 如果物件包含某個範圍內數個 IP 位址的話，請選擇**範圍位址**。 如果物件包含 IP 位址的子網路的話，請選擇**子網路位址**。 如果物件包含任何一種 IP 位址的話請選擇**任何位址**。
起始 IP 位址	輸入單一位址類型所需的起始 IP 位址。
結束 IP 位址	如果選擇的是範圍位址類型，請輸入結束 IP 位址。
子網路位址	如果選擇的是**子網路位址**類型，請輸入子網路遮罩位址。
反向選擇	如果勾選此項的話，除了上面所提及的以外，其他的 IP 位址將會在被選擇之後全部套用上設定內容。

下表爲 IP 物件設定的範例之一。

IP物件設定檔:

索引編號	名稱
1.	研發部門
2.	財務部門
3.	人資部門
4.	

3.4.2 IP 群組

本頁可讓您綁定數個 IP 物件成爲一個 IP 群組。

物件設定 >> IP 群組

IP群組表: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

回復出廠預設值　　清除全部的設定資料。

按下任一索引號碼以便完成詳細設定。

物件設定 >> IP 群組

設定檔索引號碼：1

名稱:

介面: 任何一種

可用之 IP 物件

1-研發部門
2-財務部門
3-人資部門

»
«

選定 IP 物件

確定　取消

名稱　　請輸入本設定檔的名稱，最多可以輸入 15 個字元。

介面　　請選擇適當的介面(WAN, LAN 或是任何一種)以顯示所有指定介面內的 IP 物件。

可用之 **IP** 物件　　所有選定之指定介面中可用的 IP 物件全都會顯示在此方塊中。

選定 **IP** 物件　　按下 » 按鈕來新增選定 IP 物件並呈現在此方塊內。

3.4.3 服務類型物件

您可設定 96 組不同條件的服務類型物件。

物件設定 >> 服務類型物件

服務類型物件設定檔: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 >> 下一頁 >>

回復出廠預設值　清除全部的設定資料。

按下任一索引號碼進入下述畫面：

物件設定 >> 服務類型物件設定

設定檔索引：1

名稱	
通訊協定	任何一種
來源通訊埠	= 1 ~ 65535
目標通訊埠	= 1 ~ 65535

確定 取消

名稱　輸入此設定檔的名稱。

介面　請選擇此設定檔所要套用的適當介面。

TCP 6

任何一種
ICMP
IGMP
TCP
UDP
TCP/UDP
其他

來源/目標通訊埠　來源通訊埠與目標通訊埠欄位皆為 TCP/UDP 可用之通訊埠，如果是其他的通訊協定，這些欄位即可省略，過濾器規則將可過濾任何一種通訊埠號。

(=) – 當第一與最後的數值相同時，此符號表示一個通訊埠。當第一與最後的數值不同時，此符號表示此設定檔所

適用的通訊埠號範圍。

(!=) –當第一與最後的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當第一與最後的數值不同時，此符號表示所有的通訊埠除了此處所設定的範圍以外，全都適用於此設定檔。

(>) – 大於此數值的通訊埠號皆可使用。

(<) – 小於此數值的通訊埠號皆可使用。

下表爲服務類型物件設定的範例之一。

服務類型物件設定檔:

索引編號	名稱
1.	SIP
2.	RTP
3.	
4.	

3.4.4 服務類型群組

本頁可讓您綁定數個服務類型物件成爲一個群組。

物件設定 >> 服務類型群組

服務類型群組表格:　　| 回復出廠預設值 |

群組	名稱	群組	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

回復出廠預設值	清除全部的設定資料。

按下任一索引號碼進入下述畫面：

物件設定 >> 服務類型群組設定

設定檔索引號碼：1

名稱: VoIP

可用之服務類型物件: 1-SIP, 2-RTP

選定之服務類型物件

» «

確定 取消

名稱	輸入此設定檔名稱。
可用之服務類型物件	您可以從 IP 物件頁面中先新增一些服務類型，所有可用的服務類型將會顯示在此區域中。
選定之服務類型物件	按下 » 按鈕來新增選定服務類型並呈現在此方塊內。

3.4.5 數位內容安全管理(CSM)

您可以針對不同的 IM 或是 P2P 應用程式訂定不同的原則，CSM 設定檔可以運用在過濾器設定頁面。

物件設定 >> CSM設定檔

CSM設定檔列表: | 回復出廠預設值 |

設定檔	名稱	設定檔	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

回復出廠預設值	清除全部的設定資料。

按下任一設定檔索引號碼進入下述畫面：

物件設定 >> CSM 設定檔

設定檔索引: 1

設定檔名稱

選擇不允許使用之項目

IM 即時通			VoIP
MSN	Yahoo Messenger	ICQ	jajah
AIM	QQ	iChat	Skype
Google Talk			
Web IM (http://www.e-messenger.net/)			
Web MSN (http://webmessenger.msn.com/)			

P2P 分享程式	
通訊協定	其他應用
SoulSeek	SoulSeek
eDonkey	eDonkey, eMule, Shareaza
FastTrack	KazaA, iMesh
Gnutella	BearShare, Limewire, Shareaza
BitTorrent	BitTorrent

確定 取消

設定檔名稱　　輸入 CSM 設定檔的名稱。

這裡提供了數個 IM, VoIP, P2P 常用項目作爲選項，方便使用者勾選以限制其他用戶的使用狀況。只要勾選方框然後按下**確定**鈕即可，稍後在**防火牆>>編輯過濾器設定>>編輯過濾器規則**頁面中，您可以使用內容管理下拉式選項選擇適合的 CSM 設定檔作爲主機可以依循的標準。

3.5 防火牆

3.5.1 防火牆基本常識

當寬頻使用者需要更多的頻寬以便用於多媒體、應用程式或是遠程學習時，安全性總是最受到重視的一環。Vigor 路由器的防火牆可以協助保護您本地網路免受外在人物的攻擊，同時它可限制本地網路的使用者存取網際網路。此外它還可以過濾一些由觸發路由器所建立的連線特定封包。

最基本的安全觀念就是在您安裝路由器時，設定使用者名稱和密碼。管理者登入可以防止未授權用戶從您的路由器登入並更改存取路由器設定。

快速設定精靈

輸入登入密碼

請重新輸入字母及數字組合之字串作為您的 密碼 (最大23個字元).

新密碼 ••••

確認密碼 ••••

< 上一步 | 下一步 > | 完成 | 取消

如果您在安裝時並未設定密碼，您可以至**系統維護>>系統管理員密碼設定**中設定您的密碼。

系統維護 >> 系統管理員密碼設定

系統管理員密碼

舊密碼

新密碼

確認密碼

確定

防火牆工具

區域網路上的使用者可以下述的防火牆工具，接受良好的安全防護：

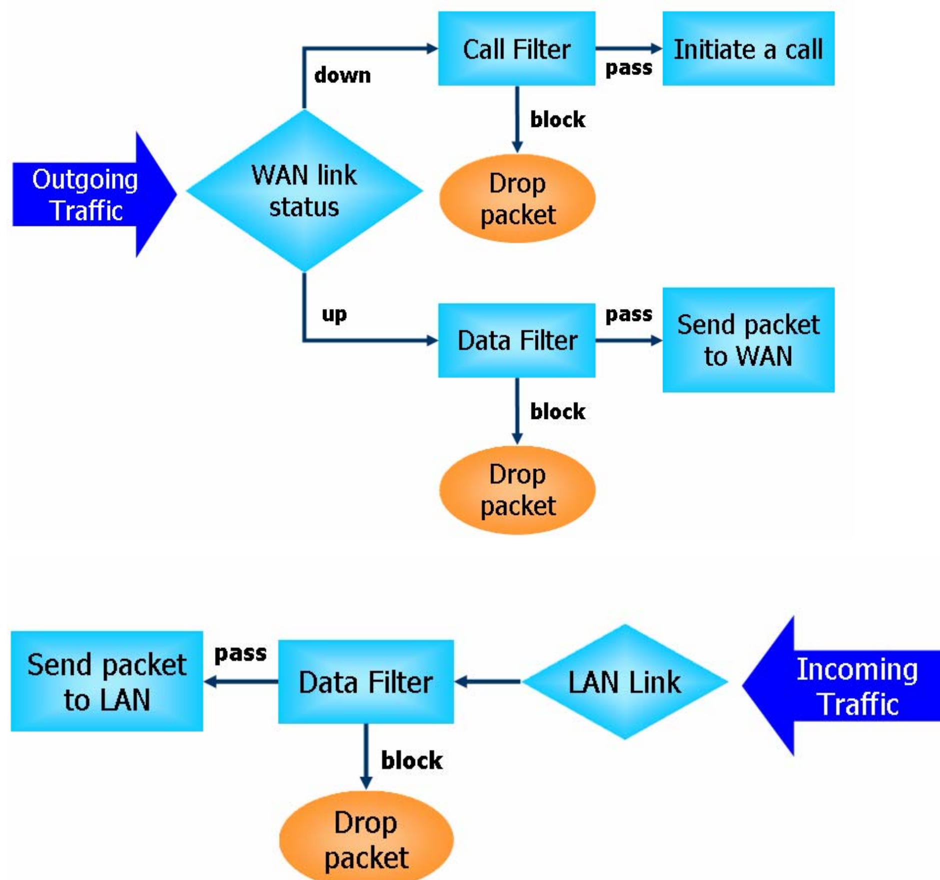
- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦
- URL 內容過濾器

IP 過濾器

依照現有網際網路連線的需求、廣域網路連接狀態(開啟或關閉)的情形，IP 過濾器結構可將資料流量分成二大類：呼叫過濾器和資料過濾器。

- **呼叫過濾器** -當目前沒有任何網際網路連線時，呼叫過濾器可應用在所有的資料運輸流量上，所有的運輸應該是往外送出。系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過，然後路由器將啟動一次呼叫來建立網際網路連線，再將該封包傳送往網際網路。
- **資料過濾器** - 網際網路正處於連線狀態時，資料過濾器可應用在流入與流出的資料傳輸上，系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過。

以下圖表解釋流入與流出之資料傳輸程序。



封包狀態檢測(SPI)

在網路層級上，封包狀態檢測是一種防火牆結構，它會建立一個封包狀態機器來追蹤防火牆於所有介面的連線狀況，並確保這些連線都是有效的。此類型防火牆並不只是檢查封包標頭資訊，它同時也監視著連線的狀態。

數位內容安全管理(Content Security Management, CSM)

因爲立即通訊應用程式蓬勃的發展，人與人間的通訊變得越來越容易。然而一些企業利用此種程式作爲與客戶通訊的有力工具時，部分公司對此可能還是抱持保留態度，這是因爲他們想要減少員工在上班時間誤用此程式或是防止未知的安全漏洞發生。對於準備應用點對點程式的公司來說，情況也是相同的，因爲檔案分享可以很方便但是同時也很危險。爲了應付這些需求，我們提供了 CSM 阻擋功能。

DoS 攻擊防禦

DoS 攻擊防禦功能協助用戶檢測並減輕 DoS 攻擊，這類攻擊通常可分成二大類 – flood 類型攻擊和弱點攻擊。flood 類型攻擊嘗試耗盡您的系統資源，而弱點攻擊則是利用通訊協定或是操作系統的弱點嘗試癱瘓系統。

DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫爲基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

Vigor 路由器也可以監視資料流量，任何違反事先定義的參數的不正常資料流(例如臨界值的數字)，都會被視爲是一種攻擊行爲，Vigor 路由器將啓動防衛機制，及時阻擋減輕災害。

下列表格顯示出 DoS 攻擊防禦功能所能檢測出的攻擊類型。:

1. SYN flood 攻擊
2. UDP flood 攻擊
3. ICMP flood 攻擊
4. TCP Flag scan
5. 路由追蹤
6. IP options
7. 未知通訊協定
8. Land 攻擊
9. Smurf 攻擊
10. SYN 封包片段攻擊
11. ICMP 封包片段攻擊
12. Tear drop 攻擊
13. Fraggle 攻擊
14. Ping of Death 攻擊
15. TCP/UDP port scan

內容過濾器

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

網頁內容過濾器

我們都知道網際網路上的內容，有時候可能並不太合宜，作為一個負責任的父母或是雇主，您應該保護那些您信賴的人免受危險的侵擾。藉由 Vigor 路由器的網頁過濾服務，您可以保護您的商業機密不受一般常見威脅；對於父母來說，您可以保護您的孩童不致誤闖成人網站或是成人聊天室。

一旦您啟動了網頁內容過濾服務，也選擇一些您想要限制存取的網站目錄，每個 URL 位址需求(例 www.bbc.co.uk) 將在由 SurfControl 所運作的伺服器資料庫中先接受檢測。資料庫涵蓋 70 種語言和 200 個國家，超過 1 億個網頁，區分成 40 種容易瞭解的目錄。此資料庫每一天都由網際網路的國際研究團隊不斷更新，伺服器將查閱 URL 然後傳回其類別給路由器，您的 Vigor 路由器即可按照您所選擇的分類項目來決定是否允許用戶存取該網站，因為每一個多路負載平衡資料庫伺服器一次可以管理數百萬的分類需求。.

下圖為防火牆的功能項目：



3.5.2 基本設定

基本設定允許您調整 IP 過濾器和一般選項的設定內容，在此頁面您可以啟動或是關閉**呼叫過濾器**或**資料過濾器**。在某些情況下，您的過濾器可利用連結的方式執行一系列過濾工作，因此在這裡，您只要指定**開始過濾器組別**即可。當然，您也可以調整紀錄模式設定以及勾選**接受流入的 UDP Fragment 封包**。

自**防火牆**群中選擇**基本設定**連結。

防火牆 >> 基本設定

基本設定

呼叫過濾器	⦿ 啟用	開始過濾器組別	組別#1
	○ 停用		
資料過濾器	⦿ 啟用	開始過濾器組別	組別#2
	○ 停用		

預設規則之動作:

應用程式	動作/設定	Log
過濾器	通過	☐
數位內容安全管理	無	☐

☐ 套用 IP 過濾器至 VPN 的輸入封包。

☑ 接受流入的大量 UDP 或是 ICMP Fragment 封包 (用於某些遊戲，如CS)

確定 清除

呼叫過濾器	選擇**啟用**以啟動呼叫過濾器功能，並指定開始過濾器組別。
資料過濾器	選擇**啟用**以啟動資料過濾器功能，並指定開始過濾器組別。

過濾器	對不符合上述的過濾器規則之封包，可以選擇讓其通過或是將之封鎖。 
數位內容安全管理	選擇**數位內容安全管理(**CSM) 設定檔作爲封鎖 IM/P2P 應用之用，區域網路上全部的主機都必須遵守 CSM 所訂的規則。詳細的資訊，請參考**數位內容安全管理(**CSM)設定檔頁面。
Log	針對疑難排解的需要，您可在此指定呈現過濾器/CSM/防毒/防駭的處理記錄，只要勾選各項目右邊的核取方塊即可。勾選了方塊可記錄所有的封包而不勾選方塊則可忽略所有的封包處理記錄，這些內容會顯示在 Draytek Syslog 視窗中。

一些線上遊戲都會使用很多的片段 UDP 封包來傳送遊戲資料，出於安全防火牆的本能直覺，Vigor 路由器會將這些片段封包給退回，以避免攻擊發生，除非您啓動**接受流入的 UDP 或是 ICMP Fragment 封包**，勾選此方塊後，您就可以悠遊這些線上遊戲。如果安全性具有較高重要性，請勿啓動**接受流入的 UDP 或是 ICMP Fragment 封包**功能。

3.5.3 過濾器設定

按防火牆並選擇**過濾器設定**以開啓如下的設定網頁。

防火牆 >> 過濾器設定

過濾器設定 | 回復出廠預設值 |

組別	註解	組別	註解
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

如果要新增一個過濾器，請按組別下方的數字按鈕以便編輯個別設定。如下的頁面將立即出現，每一個過濾器都含有 7 組規則，請按規則按鈕編輯每個規則，勾選**啓用**則可啓動該項規則。

防火牆 >> 過濾器設定 >>編輯過濾器設定

過濾器組別 1

註解: Default Call Filter

過濾器規則	啟用	註解	上移	下移
1	☑	Block NetBios		下
2	☐		上	下
3	☐		上	下
4	☐		上	下
5	☐		上	下
6	☐		上	下
7	☐		上	

下一個過濾器組別 無

確定 清除 取消

過濾器規則	請按號碼按鈕 (1 ~ 7) 編輯過濾器的規則，按下此鈕可以開啓過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。
啓用	啓動或是關閉此項過濾規則。
註解	輸入過濾規則註解說明，最大長度可以達到 23 個字元。
上移/下移	使用上下連結來移動過濾器規則的順序。
下一個過濾器組別	設定前往下一個執行的過濾器連結，請勿讓多個過濾器設定形成一個迴路。

欲編輯**過濾器規則**，請按過濾器規則索引按鈕以便進入過濾器規則設定網頁。

防火牆 >> 編輯過濾器設定 >> 編輯過濾器規則

過濾器組別 1 規則 1

☑ 啟用過濾規則

註解: Block NetBios

索引號碼(1-15) 於 排程 設置: , , ,

方向: LAN -> WAN

來源 IP: Any 編輯

目標 IP: Any 編輯

服務類型: TCP/UDP, Port: from 137~139 to any 編輯

片段: 忽略

應用程式	動作/設定	Syslog
過濾器:	立刻封鎖	☐
分至其他過濾器設定	無	
數位內容安全管理:	無	☐

確定 清除 取消

啓用過濾規則　　勾選此項目以啓動過濾規則。

註解　　輸入過濾器設定註解說明，最大長度爲 14 個字元。

索引號碼 (1-15)　　設定區域網路上的電腦工作的時間間隔，您可以輸入四組時間排程，所有的排程都可在**其他應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

方向　　設定封包流向的方向(LAN->WAN/WAN->LAN)，此項設定僅適用**資料過濾器**，對於**呼叫過濾器**而言，這項設定是不適用的。

來源/目標 IP　　按下**編輯**進入如下的畫面，選擇來源/目標 IP 或是一段 IP 範圍。

http://192.168.1.1 - IP 位址編輯 - Microsoft Internet Explorer

IP 位址編輯

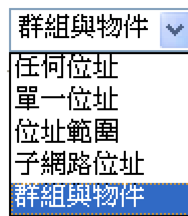
位址形式	任何位址
起始IP位址	0.0.0.0
結束IP位址	0.0.0.0
子網路遮罩	0.0.0.0
反向選擇	☐
IP 群組	無
或 IP物件	無
或 IP 物件	無
或 IP 物件	無

確定 關閉

完成　　網際網路

欲手動設定 IP 位址，請選擇任**何位址/單一位址/位址範圍/子網路位址**作爲位址形式，並在此畫面輸入相關內容，此外如果您想要使用群組或是物件中所定義的 IP 範圍，請選擇**群組與物件**

作爲位址形式。

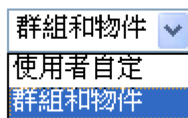


請自下拉式選項中選擇您需要的形式，或是使用 IP 物件下拉式選項挑選所需的物件。

服務類型 按**編輯**進入如下的畫面，以選擇適合之服務類型。



欲手動設定服務類型，請選擇使用者自訂做爲服務類型，並輸入相關的設定資料，此外如果您想要使用群組或是物件中所定義的服務類型，請選擇**群組與物件**作爲服務類型。



協定 -指定本過濾器規則套用的協定。
來源/目標通訊埠 -
(=) – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。
(!=) –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。
(>) – 大於此數值的通訊埠號皆可使用。
(<) – 小於此數值的通訊埠號皆可使用。
服務群組/物件 - 使用下拉式選項選擇所需的項目。

片段	指定片段封包的執行動作，這個項目也是僅針對**資料過濾器**。 **忽略** - 不論是怎樣的片端封包，系統皆不採取行動。 **無片段** - 應用規則至無片段之封包上。 **片段**- 應用規則至片段之封包上。 **太短了** - 只有過短無法包含完整封包頭之封包，可應用此規則。
過濾器	指定系統針對符合規則之封包所採取的行動。 過濾器: 立刻封鎖 立刻通過 立刻封鎖 若無符合其餘規則即通過 若無符合其餘規則即封鎖 **立刻通過**- 符合規則之封包可立即通過。 **立刻封鎖** - 系統封鎖符合規則之封包。 **若無符合其於規則即通過** - 符合限定規則且並未符合其他規則之封包可立即通過。 **若無符合其於規則即封鎖** - 系統封鎖符合限定規則且並未符合其他規則之封包。
分至其他過濾器設定	封包符合過濾器規則，下一個過濾器規則將分至指定之過濾器設定。請自下拉式選項中選擇下一個過濾器規則以便做分支動作，要注意路由器將會採用指定之過濾器規則，且絕對不會回到先前所設定之過濾器規則。
Syslog	針對疑難排解的需要，您可在此指定呈現過濾器/CSM/防毒/防駭的處理記錄，只要勾選各項目右邊的核取方塊即可。勾選了方塊可記錄所有的封包而不勾選方塊則可忽略所有的封包處理記錄，這些內容會顯示在 Draytek Syslog 視窗中。
數位內容安全管理	上述條件下設定範圍中的全部主機都必須遵守 CSM 設定檔中的標準，詳細資訊請參考 CSM 一節。

範例

如前所言，全部的資料傳輸都將以二種 IP 過濾器(呼叫過濾器或是資料過濾器）來分開執行，您可以設定 12 組呼叫過濾器和資料過濾器，每種過濾器設定由 7 種過濾器規則組合而成，這些規則都是事前定義完成。然後在**基本設定**中， 您可以指定一組規則予呼叫過濾器與資料過濾器使用。

防火牆 >> 基本設定

基本設定

呼叫過濾器	⦿ 啟用 ○ 停用	開始過濾器組別 組別#1
資料過濾器	⦿ 啟用 ○ 停用	開始過濾器組別 組別#2

預設規則之動作:

應用程式	動作/設定	Log
過濾器	通過	☐
數位內容安全管理	無	☐

☐ 套用 IP 過濾器至 VPN 的輸入封包。

☑ 接受流入的大量 UDP 或是 ICMP Fragment 封包 (用於某些遊戲，

確定 清除

防火牆 >> 過濾器設定

過濾器設定 | 回復出廠預設值 |

組別	註解	組別	註解
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

防火牆 >> 過濾器設定 >> 編輯過濾器設定

過濾器組別 1

註解: Default Call Filter

過濾器規則	啟用	註解
1	☑	Block NetBios
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	

確定 清除 取消

防火牆 >> 編輯過濾器設定 >> 編輯過濾器規則

過濾器組別 1 規則 1

☑ 啟用過濾規則

註解: Block NetBios

索引號碼(1-15) 於 排程 設置:

方向: LAN -> WAN

來源 IP: Any 編輯

目標 IP: Any 編輯

服務類型: TCP/UDP, Port: from 137~139 to any 編輯

片段: 忽略

應用程式	動作/設定	Syslog
過濾器:	立刻封鎖	☐
分至其他過濾器設定	無	
數位內容安全管理:	無	☐

確定 清除 取消

3.5.4 DoS 攻擊防禦功能設定

這是 **IP 過濾程式/防火牆**的次功能選項，有 15 種檢測/防禦功能類型，DoS 攻擊防禦功能的預設值是關閉的。

按防火牆並選擇 **DoS 攻擊防禦功能**開啓設定網頁。

防火牆 >> DoS 攻擊防禦功能設定

DoS 攻擊防禦功能設定

☑ 啟用 DoS 防禦功能

☐ 啟用 SYN flood 攻擊防禦功能	臨界值	50	封包 / 秒
	逾時	10	秒
☐ 啟用 UDP flood 攻擊防禦功能	臨界值	150	封包 / 秒
	逾時	10	秒
☐ 啟用 ICMP 攻擊防禦功能	臨界值	50	封包 / 秒
	逾時	10	秒
☐ 啟用防禦通訊埠掃瞄偵測功能	臨界值	150	封包 / 秒

☐ 封鎖 IP options	☐ 封鎖 TCP Flags scan
☐ 封鎖 Land 攻擊	☐ 封鎖 Tear Drop 攻擊
☐ 封鎖 Smurf 攻擊	☐ 封鎖 Ping of Death 攻擊
☐ 封鎖路由追蹤（Trace Route）	☐ 封鎖 ICMP 封包片段攻擊
☐ 封鎖 SYN Fragment 封包	☐ 封鎖不明封包協定封包
☐ 封鎖 Fraggle 攻擊	

啟用抵擋DoS攻擊功能，防止外來駭客攻擊。

確定　全部清除　取消

啓用　勾選此項以啓動 DoS 攻擊防禦功能。

啓用 SYN flood 攻擊防禦功能　勾選此項以啓動 SYN 攻擊防禦功能，一旦檢查到 TCP SYN 封包的臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 TCP SYN 封包，這項功能的目的是防止 TCP SYN 封包嚐試耗盡路由器有限的資源。臨界值和逾時的預設值分別爲每秒 50 個封包和 10 秒。

啓用 UDP flood 攻擊防禦功能　勾選此項以啓動 UDP 攻擊防禦功能， 一旦檢查到 UDP 封包臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 UDP 封包。臨界值和逾時的預設值分別爲每秒 150 個封包和 10 秒。

啓用 ICMP flood 攻擊防禦功能　勾選此項以啓動 ICMP 攻擊防禦功能，與 UDP 攻擊防禦功能相同的是，一旦檢查到 ICMP 封包臨界值超過定義數值，路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP 需求。臨界值和逾時的預設值分別爲每秒 50 個封包和 10 秒。

啓用防禦通訊埠掃瞄偵測功能　通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意

探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的預設值爲每秒 150 個封包。

封鎖 **IP options**	勾選此項以啓動阻攔 IP options 功能，Vigor 路由器將會忽略資料封包頭中(含 IP 選項區)的 IP 封包。限制的原因是 IP option 的出現是區域網路安全性中的弱點，因爲它攜帶令人注意的資訊像是安全性、TCC (封閉使用者群組)參數、網際網路位址、路由訊息等等，讓外部的竊聽者有機會取得您虛擬網路的細節內容。
封鎖 **Land** 攻擊	勾選此項以強迫 Vigor 路由器防護 Land 攻擊，Land 攻擊結合含 IP spoofing 的 SYN 攻擊技術，當駭客傳送 spoofed SYN 封包(連同相同來源和目的位址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。
封鎖 **Smurf** 攻擊	勾選此項以啓動封鎖 Smurf 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。
封鎖路由追蹤	勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。
封鎖 **SYN Fragment** 封包	勾選此項以啓動封鎖 SYN Fragment 的封包功能。Vigor 路由器將會停止任何具有 SYN 旗標及更多的區段設定之封包傳送作業。
封鎖 **Fraggle** 攻擊	勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。 啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。
封鎖 **TCP Flags scan**	勾選此項以啓動阻攔 TCP Flags 掃描功能，任何具有異常 TCP 封包的設定都會被捨棄掉，這些掃描行動包含有 *no flag scan, FIN without ACK scan, SYN FINscan, Xmas scan* 以及 *full Xmas scan* 等等。
封鎖 **Tear Drop** 攻擊	勾選此項以啓動封鎖 Tear Drop 攻擊功能，很多機器在接收到超過最大值得 ICMP 資料段(封包)時，系統就會當機。爲了避免這類型的攻擊行爲，Vigor 路由器便被設計成具有捨棄片段 ICMP (超過 1024 位元組)封包的能力。
封鎖 **Ping of Death** 攻擊	勾選此項以啓動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。
封鎖 **ICMP** 封包片段攻擊	勾選此項以啓動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。
封鎖不明封包協定封包	勾選此項以啓動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。

警告訊息

我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作爲系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。

所有與 DoS 攻擊有關的警告訊息都將傳送與使用者，使用者可以重新檢查其內容，在訊息中尋找關鍵字，所遭受的任何攻擊之名稱即可立即檢測出來。

系統維護 >> Syslog / 郵件警示設定

Syslog / 郵件警示設定

Syslog 存取設定		郵件警示功能設定	
☑ 啟用		☐ 啟用	
伺服器 IP 位址		SMTP 伺服器	
目標通訊埠	514	收件人	
啟用 Syslog 訊息:		回信地址	
☑ 防火牆記錄		☐ 驗證	
☑ VPN 記錄		使用者名稱	
☑ 使用者網路存取紀錄		密碼	
☑ 通話紀錄			
☑ WAN 記錄			
☑ 路由器/DSL資訊			

確定 清除 取消

DrayTek Syslog

Controls: 192.168.1.1 — Vigor3100 series Dmt.Bis

LAN Status

TX Packets	RX Packets
931	1182

WAN Status

Getway IP (Fixed)	TX Packets	RX Rate
---	0	0
WAN IP (Fixed)	RX Packets	TX Rate
---	0	0

Firewall Log | VPN Log | User Access Log | Call Log | WAN Log | Budget Log | Network Infomation | Net State

Time	Host	Message
Jan 1 00:00:42	Vigor	DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 3943751
Jan 1 00:00:34	Vigor	DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
T1.413	HANDSHAKE	0	0	0.0	0.0

3.5.5 URL 內容過濾器

基於使用者定義的關鍵字清單，Vigor 路由器中的 URL 內容過濾器對每一次的外送 HTTP 需求，都會執行檢測 URL 字串的動作，不論該字串是部分還是全部符合關鍵字的設定，Vigor 路由都將會阻擋相關聯的 HTTP 連線。

例如，假設您新增關鍵字是“sex (性)”，路由器即會限制進入某些網頁或是網站存取的功能，比方 www.sex.com、www.backdoor.net/images/sex/p_386.html，或者您也可以指定 URL 全名或部分的名稱如 www.sex.com 或是 sex.com 來加以限制。

按防火牆並選擇 **URL 內容過濾器**開啓設定網頁。

防火牆 >> URL內容過濾器

內容過濾器設定

☑ 啟用URL存取控制

☐ 啟用URL存取紀錄

◉ 黑名單 (封鎖符合關鍵字之網頁)

○ 白名單(放行符合關鍵字之網頁)

號碼	啟用	關鍵字	號碼	啟用	關鍵字
1	☐		5	☐	
2	☐		6	☐	
3	☐		7	☐	
4	☐		8	☐	

空白處可同時指定多個關鍵字。例如: hotmail yahoo msn

☐ 防止透過IP位址對網站進行存取

☐ 啟用有限網站功能

☐ Java ☐ ActiveX ☐ 壓縮檔 ☐ 執行檔 ☐ 多媒體檔案

☐ Cookie ☐ 伺服器

☐ 啟用子網路功能

號碼	啟用	IP位址		子網路遮罩
1	☐		~	
2	☐		~	
3	☐		~	
4	☐		~	

排程

索引(1-15)於 排程 設定: , , ,

附註: 排程設定中之動作與閒置逾時欄位不適用於此。

確定 全部清除 取消

啓用 URL 存取控制	勾選此項啓動 URL 存取控制。
啓用 URL 存取紀錄	勾選此項啓動 URL 存取紀錄。
黑名單(封鎖符合關鍵字之網頁)	按此鈕限制下述清單中所列關鍵字之相關網頁的存取。
白名單(放行符合關鍵字之網頁)	按此鈕允許下述清單中所列關鍵字之相關網頁的存取。
關鍵字	Vigor 路由器提供 8 個關鍵字設定欄位以定義關鍵字，每個欄位都支援數個關鍵字設定。關鍵字可以是名詞、名詞的部份片

段、或是完整的 URL 字串。欄位中的多重關鍵字以空格、逗號或是分號來區分，此外每個欄位的最大長度爲 32 個文字。指定完關鍵字之後，Vigor 路由器將降低 URL 字串符合使用者自定關鍵字的網站之連線需求。要注意的是阻擋關鍵字清單越是簡化，Vigor 路由器處理得就越有效率。

防止透過 **IP** 位址對網站進行存取	勾選此項以防止一些利用 IP 位址(如 http://202.6.3.2)執行搜尋之動作，其目的是在預防某些人閃避 URL 存取控制。 首先您必須清除瀏覽器快取，這樣 URL 內容過濾器才能合宜的在您之前造訪過的網頁上操作。
啓用有限網站功能	勾選此方塊啓動此功能。 ***Java -*** 勾選此方塊啓動阻擋 Java 物件功能，Vigor 路由器將會從網際網路上捨棄 Java 物件。 ***ActiveX*** - 勾選此方塊啓動 Block ActiveX 物件功能，任何來自網際網路的 ActiveX 物件都會被擋掉。 *壓縮檔* - 勾選此方塊啓動**壓縮檔**物件功能，防止他人下載任何壓縮的檔案，下列清單顯示可被路由器阻擋的壓縮檔案類型： **zip, rar, .arj, .ace, .cab, .sit** *執行檔* -勾選此方塊拒絕任何來自網際網路執行檔的下載行爲。 **.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg** ***Cookie - -***勾選此方塊過濾由內而外的 cookie 傳送，以保護本地用戶的隱私。 ***Proxy --***勾選此方塊拒絕任何的代理傳送，如果要有效控制頻寬用途，那麼過濾多媒體檔案網路之下載之阻擋機制，就有很大的價值了，相對來說，下述所列之檔案格式都可被 Vigor 路由器阻擋在外。 **.mov .mp3 .rm .ra .au .wmv** **.wav .asf .mpg .mpeg .avi .ram**
封鎖子網路功能	使用者可以指定特定 IP 位址或是子網路免受 URL 存取控制，共可輸入四個 IP 位址，欲啓動每一項設定，請勾選前面的**啓用**方塊。
排程	指定某個時段執行 URL 內容過濾。

3.5.6 網頁內容過濾器

按**防火牆**並選擇**網頁內容過濾器**開啓設定網頁。

有關本節詳細資訊，請參考**網頁內容過濾器**使用手冊。

防火牆 >> 網頁內容過濾設定

CPA(Content Portal Authority) 網頁內容過濾程式

選擇任一CPA伺服器: asia site

開始試用/購買服務
檢查有效性
測試網站以驗證該站是否已歸類

☐ **啟用網頁內容過濾程式**

群組	分類（請勾選需封鎖的分類）		
未成年保護 [全選] [全部清除]	☐聊天	☐犯罪	☐藥物/酒
	☐賭博	☐駭客	☐貶損言論
	☐性	☐暴力	☐武器
休閒 [全選] [全部清除]	☐廣告	☐娛樂	☐美食
	☐遊戲	☐魅力	☐健康
	☐嗜好	☐生活	☐汽車/重機車
	☐個人	☐照片搜尋	☐購物
	☐運動	☐影音	☐旅行
財經 [全選] [全部清除]	☐電腦/網際網路	☐金融	☐工作
	☐政治	☐房地產	☐參考資料
	☐遠端伺服器	☐搜尋引擎	☐Web 郵件
其它 [全選] [全部清除]	☐教育	☐網站要塞	☐孩童網站
	☐新聞	☐信仰	☐性教育
	☐部落格/論壇/新聞群組	☐封鎖所有未分類的網站	

排程

索引(1-15)於 **排程** 設定: [ ], [ ], [ ], [ ]

附註: 排程設定中之動作與閒置逾時欄位不適用於此。

[確定] [取消]

3.6 頻寬管理

下面是頻寬管理的設定項目:



3.6.1 NAT 連線數限制

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer) 應用程式(如 BitTorrent)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。為了解決這種問題，您可以使用連線數限制來限制指定主機的連線數。

在**頻寬管理**群組中，按**連線數限制**開啓如下的網頁。

頻寬管理 >> NAT 連線數限制

NAT 連線數限制

○ 啟用 ◉ 停用

預設最大連線數: 100

限制清單

索引	起始 IP	結束 IP	最大連線數

指定限制

起始 IP: 結束 IP:

最大連線數

新增 編輯 刪除

時間排程

索引號碼(1-15)於 排程 設定: , , ,

附註: 排程設定中之動作與閒置逾時欄位不適用於此。

確定

如果要啓動限制連線數的功能，只要在此頁面上按**啓用**鈕，並設定預設的連線數限制即可。

啓用	按此鈕啓動連線數限制功能。
停用	按此鈕關閉連線數限制功能。
預設最大連線數	定義區域網路中每台電腦的預設連線數。
限制清單	顯示網頁中所設定的指定限制之電腦清單資料。
起始 IP	定義連線數限制的起始 IP 位址。
結束 IP	定義連線數限制的結束 IP 位址。
最大連線數	定義指定 IP 位址的範圍中每個 IP 可用的連線數，若您未設定連線數，系統將使用預設連線數值(10000)。

新增	新增指定連線數限制並顯示在上面的框框中。
編輯	允許您編輯選定的連線數設定。
刪除	刪除限制清單上任何一個您所選定的設定。
索引號碼(1-15)於排程設定..	您可以輸入四組時間排程，所有的排程都可在**其他應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

3.6.2 頻寬限制

從 FTP,HTTP 或是某些 P2P 應用程式的下行或上行資料會佔據很大的頻寬，並影響其他程式的運作。請使用限制頻寬讓頻寬的應用更有效率。

在**頻寬管理**群組中，按**頻寬限制**開啓如下的網頁。

頻寬管理 >> 頻寬限制

頻寬限制

○ 啟用 ⊙ 停用

預設傳送限制: 200 Kbps 預設接收限制: 800 Kbps

限制清單

索引編號	起始 IP	結束 IP	傳送限制	接收限制

指定限制

起始 IP: 結束 IP:

傳送限制: Kbps 接收限制: Kbps

新增 編輯 刪除

時間排程

索引號碼(1-15) 於 排程 設定: , , ,

附註: 排程設定中之動作與閒置逾時欄位不適用於此。

確定

如果要啓動限制頻寬的功能，只要在此頁面上按**啓用**鈕，並設定預設的上下行資料傳送限制即可。

啓用	按此鈕啓動限制頻寬功能。
停用	按此鈕關閉限制頻寬功能。
預設傳送限制	定義區域網路中每台電腦預設的上行速度。
預設接收限制	定義區域網路中每台電腦預設的下行速度。
限制清單	顯示網頁中所設定的指定限制之電腦清單資料。
起始 IP	定義限制頻寬的起始 IP 位址。
結束 IP	定義限制頻寬的結束 IP 位址。

傳送限制	定義上行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。
接收限制	定義下行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。
新增	新增指定速度限制並顯示在上面的框框中。
編輯	允許您編輯選定的限制設定。
刪除	刪除限制清單上任何一個您所選定的設定。
索引號碼(1-15)於排程設定..	您可以輸入四組時間排程，所有的排程都可在**其他應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

3.6.3 服務品質(QoS)

QoS (Quality of Service)管理部署可確保所有應用程式能夠接收到所需的服務以及足夠的頻寬，符合用戶所期待的效果，此項控制對現代企業網路來說是相當重要的觀點。

使用 QoS 的理由之一是很多 TCP 為主的應用程式嘗試不斷增加其傳輸速率，導致消耗掉全部的頻寬，我們稱之為 TCP 慢速啓動。如果其他的應用程式未受 QoS 的保護，那麼他們在擁擠的網路中將會降低效能，對那些無法忍受任何損失、延遲的功能像是 VoIP、視訊會議以及流動影像來說，這項控制尤其必要。

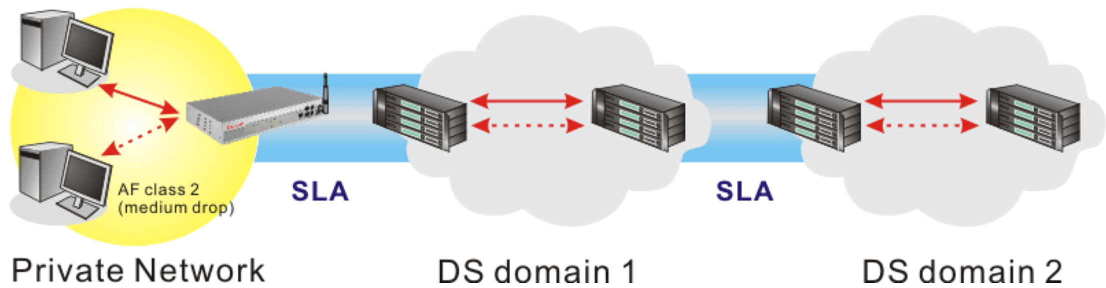
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成為被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

在基本設定中有二個元件要注意：

- 分類: 可辨識低潛在因素或是重要的應用程式，並標示這些程式為高優先權服務等級，以便在網路中能夠強迫執行。
- 排定計畫: 以服務等級分類為基礎來指定封包排列順序以及整合的服務型態。

基本 QoS 應用是以 IP 封包頭中之服務類型資訊為基礎來分類及規劃封包，例如為了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

Vigor 路由器作為 DS 管理之終端路由器，應該檢查通過流量之 IP 封包頭中標記 DSCP 之數值，這樣才可分配特定資源數量來執行適當政策、分類或是排程。網路骨幹之核心路由器在執行動作前也會做同樣的檢查，以確保整個 QoS 啓動之網路中服務等級保持一致性。



QoS 將以上傳/下載速度比率來定義，我們也會提供一些 QoS 需求應用給您參考，設定數值會依照網路實際狀況而有所改變。

在**頻寬管理**群組中，選擇**服務品質**開啓如下的網頁。

頻寬管理 >> 服務品質(QoS)

基本設定

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	
WAN1	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定
WAN2	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

本頁顯示 WAN 介面上的 QoS 設定成果，按下設定連結進入下一層頁面，至於類別規則，則按下該頁面上的**編輯**按鈕進入另一層畫面來設定即可。

您可以設定 WAN 介面的一般設定，並視您的需要來編輯類別規則並且編輯類別規則的服務類型。

WAN 基本設定

當您按下設定時，您可調整 WAN 介面的 QoS 頻寬比率，系統提供您四種類別作為 QoS 控制之用，前三種(類別 1 到類別 3)可視您的需求來調整，而最後一個則保留給那些不符合上面定義之規則等封包使用。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

☑ 啟用服務品質(QoS)控制功能 上傳

WAN 下載頻寬	10000	Kbps
WAN 上傳頻寬	10000	Kbps

索引編號	類別名稱	保留頻寬比例
類別 1		25 %
類別 2		25 %
類別 3		25 %
	其他	25 %

☑ 啟用 UDP 頻寬控制　　頻寬限制比率 25 %

連線狀態統計

確定　清除　取消

啓用服務品質(QoS)控制　預設狀態下，這個功能是啓用的。
請同時定義 QoS 控制設應所應用的流量方向。
下載- 僅適用於進入的封包。
上傳- 僅適用於輸出的封包。
雙向- 適用於進入與輸出的封包。
勾選此方塊並按下**確定**，**連線狀態統計**連結即可出現在此頁面上。

WAN 下載頻寬　允許您設定 WAN 資料輸入的連線速度。

WAN 上傳頻寬　允許您設定 WAN 資料輸入的連線速度。
例如，您的 ADSL 支援 1M 的下行與 256K 上行速度，請將 **WAN 下載頻寬**設定為 1000kbps 而 **WAN 上傳頻寬**設定為 256kbps。

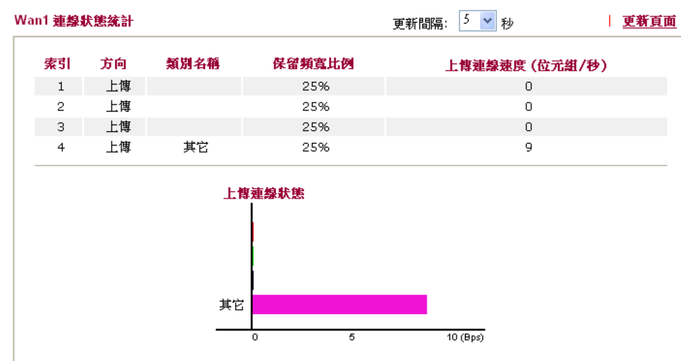
保留頻寬比例　保留作為群組索引所可應用的比率。

啓用 UDP 頻寬控制　勾選此設定並在右邊設定限制的頻寬比率，這是 TCP 應用的一種保護機制，因為 UDP 應用程式會消耗很多的頻寬。

限制頻寬比率　此處所輸入的比率保留作為 UDP 應用之需。

連線狀態統計

顯示服務品質的連線狀態統計圖供使用者參考。
這個連結只有在您於 WAN1/WAN2 **基本設定**網頁中按下**確定**按鈕，然後又到**頻寬管理>>服務品質**在按一次設定後才會出現。



編輯 Qos 的類別規則

前三種(類別 1 到類別 3)可視您的需求來調整，編輯或是刪除類別規則，請按該項類別的索引連結即可。

頻寬管理 >> 服務品質(QoS)

基本設定

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	
WAN1	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定
WAN2	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	編輯
類別 2		編輯	
類別 3		編輯	

在您按下索引連結之後，您可以看到如下的頁面。現在您可以定義該類別的名稱，在本例中，TEST 用來作爲類別 1 的名稱。

頻寬管理 >> 服務品質

類別索引#1

名稱 test

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1	空白	-	-	-	-

新增 編輯 刪除

確定 取消

若要新增一個新的規則，請按**新增**開啓下列畫面。

頻寬管理 >> 服務品質

編輯規則

☑ 啟用

本機地址　Any　編輯

遠端位址　Any　編輯

DiffServ CodePoint　ANY

服務類型　ANY

附註：請先選擇/設定 服務類型！

確定　取消

啓用　　勾選此方塊啓用本頁的設定。

本機位址　　按**編輯**按鈕以設定規則的來源位址。

遠端位址　　按**編輯**按鈕以設定規則的目標位址。

編輯按鈕　　此按鈕可讓使用者編輯來源/目標位址的範圍。



位址類型 – 決定來源位址的位址類型。
關於**單一位址**，您可以填入起始 IP 位址。
關於**範圍位址**，您必須填入起始和終點 IP 位址。
關於**子網路位址**，您必須填入起始 IP 位址和子網路遮罩。

DiffServ CodePoint　　所有的資料封包將會被切割成不同等級，並且依照系統的等級層別來處理資料封包。請指定資料所需的層級作爲 QoS 控制之用。

服務類型　　決定 QoS 控制處理時資料的服務類型，這項類型可以視情況編輯改變，您可以從下拉式選項中選擇事先定義的服務類型，這些類型都是出廠時即設定好的類型，請自行挑選一種想要使用的類型。

另外，您可以爲一種類別指定 20 組規則，如果您想要編輯現存的規則，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該規則。

頻寬管理 >> 服務品質

類別索引#1

名稱 Test

編號	狀態	來源位址	目標位址	DiffServ CodePoint	服務類型
1 ○	啟用	任何一種	任何一種	IP precedence 2	
2 ○	啟用	任何一種	任何一種	AF Class1 (Low Drop)	

新增 編輯 刪除

確定 取消

編輯類別規則的服務類型

要新增、編輯或刪除服務類型，請按服務類型區域下方的**編輯**連結。

頻寬管理 >> 服務品質(QoS)

基本設定

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	
WAN1	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定
WAN2	停用	10000Kbps/10000Kbps		25%	25%	25%	25%	不啟用	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

在您按下**編輯**按鈕之後，下面的畫面將會出現。

頻寬管理 >> 服務品質 (QoS)

使用者自訂服務類型

編號	名稱	通訊協定	通訊埠
1	空白	-	-

新增 編輯 刪除

取消

新增一個規則請按下**新增**按鈕開啓設定頁面，如果您想要編輯現有的服務類型，請選擇該項並按下**編輯**連結開啓如下頁面：

頻寬管理 >> 服務品質

編輯服務類型

服務名稱	
服務類型	TCP 6
通訊埠組態	
類型	◉ 單一 ○ 範圍
通訊埠號	0 - 0

確定 取消

服務名稱	輸入新的服務名稱。
服務類型	請選擇新服務所需的類型(TCP, UDP or TCP/UDP)。
通訊埠組態	按**單一**或是**範圍**，如果您選擇的是範圍，您必須輸入起始通訊埠號和結束通訊埠號。 **通訊埠號** –如果您選擇範圍爲服務類型，請在此輸入起始和結束通訊埠號。

另外，您可以指定 40 組服務類型，如果您想要編輯或是刪除現存的服務類型，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該服務類型。

3.7 其他應用

下圖顯示應用的功能項目：



3.7.1 動態 DNS

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網域名稱給予浮動廣域網路 IP 位址。它允許路由器線上更新廣域網路 IP 位址，以便對應至特定的 DDNS 伺服器上。一旦路由器連上網路，您將能夠使用註冊的網域名稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

在您使用 DDNS 時，您必須先向 DDNS 服務供應商要求免費的 DDNS 服務，路由器提供分別來自不同 DDNS 服務供應商的三種帳號。基本上，Vigor 路由器和大多數的 DDNS 服務供應商 **www.dyndns.org, www.no-ip.com**、**www.dtdns.com**、**www.changeip.com**、**www.dynamic-nameserver.com** 像是都能相容，您應該先造訪其網站為您的路由器註冊自己的網域名稱。

啟動此功能並增加一個動態 **DNS** 帳戶

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱為 *test*；密碼為: *test*。
2. 自**其他應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

其他應用 >> 動態 DNS 設定

動態 DNS 設定 | 回復出廠預設值 |

☐ 啟用動態 DNS 設定 [檢視記錄] [強迫更新]

帳號：

索引編號	WAN 介面	網域名稱	啟用
1.	WAN1 優先	.	x
2.	WAN1 優先	.	x
3.	WAN1 優先	.	x

[確定] [全部清除]

回復出廠預設值	清除全部設定資料並回復到出廠的設定。
啟用動態 **DNS** 設定	勾選此方塊啟用此功能。
索引編號	按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。
WAN 介面	顯示用來存取網際網路的 WAN 介面。
網域名稱	顯示您在 DDNS 設定頁面上所設定的網域名稱。

啓用	顯示此帳號目前是啓用或是停用狀態。
檢視記錄	可開啓另一個對話盒並顯示 DDNS 資訊紀錄。
強迫更新	按此按鈕強迫路由器取得最新的 DNS 資訊。

3. 選擇索引號碼 1，爲您的路由器新增一個帳號。勾選**啓用動態 DNS 帳號**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。

其他應用 >> 動態 DNS 設定>> 動態 DNS 帳號設定

索引編號: 1

☑ 啟用動態 DNS 帳號

WAN 介面	WAN1 優先
服務供應商	dyndns.org (www.dyndns.org)
服務類型	動態
網域名稱	chronic6653 . dyndns.org dyndns.org
登入名稱	chronic6653 (最多23個字元)
密碼	●●●●●●●●●●●● (最多23個字元)
☐ 萬用字元	
☐ 備份 MX	
郵件延伸程式	

確定　清除　取消

啓用動態 DNS 帳號	勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓動欄位出現勾選標示。
WAN 介面	選擇適合的介面以套用相關設定。
服務供應商	爲此 DDNS 帳號選擇適當的服務供應商。
服務類型	選擇服務類型(動態、自訂、固定)。如果您選擇的是**自訂**，您可以修正網域名稱區域中所選定的網域資料。
網域名稱	輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。
登入名稱	輸入您在申請網域名稱時所設定之登入名稱。
密碼	輸入您在申請網域名稱時所設定之密碼。
郵件延伸程式	某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件地址，以配合該 DDNS 伺服器之需要。

4. 按**確定**按鈕啓動此設定，您將會看到所做的設定已被儲存。

萬用字元與**備份 MX** 並非所有的動態 DNS 服務商都有支援，有關此部分內容，請您自服務商的網站上取得更詳盡的資訊。

關閉此功能並清除全部動態 DNS 帳號

取消勾選**啓用動態 DNS 帳號**，並按下**清除全部**按鈕停用此功能以及清除路由器內所有的帳號。

刪除動態 DNS 帳號

在**動態 DNS 設定**頁面上，請按您想要刪除之帳號的索引號碼，然後按**清除全部**按鈕即可刪除該帳號。

3.7.2 排程

Vigor 路由器可允許您手動更新，或利用網路時間協定(NTP)更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

您必須在設定排程前先設定好時間，在**系統維護**群組中，選擇**時間和日期**以開啓時間設定頁面，按**取得時間**按鈕取得與電腦(或網際網路)一致的時間，一旦您關閉或是重新啓動路由器，時鐘的時間也會重新啓動。還有另一種方法可以設定時間，您可以在網際網路上請求 NTP 伺服器(這是一個時間伺服器)以同步化路由器的時鐘，這個方法只能在廣域網路連線建立時才能使用。

其他應用 >> 排程

排程: | 回復出廠預設值 |

索引編號	狀態	索引編號	狀態
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

狀態: v --- 啟用, x --- 不啟用

回復出廠預設值	清除全部設定資料並回復到出廠的設定。
索引編號	按下方的號碼進入排程設定頁面。
狀態	顯示排程設定是啓動還是關閉。

您最多可以設定 15 個排程，然後可以應用於**網際網路連線控制**或是 **VPN** 的**遠端存取控制 LAN-to-LAN** 設定上。

欲新增一個排程，請按任何一個索引號碼，這裡舉索引編號 1 爲例。其呼叫排程的細部設定顯示如下：

其他應用 >> 排程

索引編號 1

☑ 啟用排程設定

開始日期 (yyyy-mm-dd) 2000 - 1 - 1

開始時間 (hh:mm) 0 : 0

持續時間 (hh:mm) 0 : 0

動作 強迫啟用

閒置逾時 0 分鐘。(最大值255，預設值0)

頻率

○ 一次

◉ 週期

☐ 週日 ☑ 週一 ☑ 週二 ☑ 週三 ☑ 週四 ☑ 週五 ☐ 週六

確定 清除 取消

啓用排程設定	勾選此項目以啓動此排程。
開始日期 (yyyy-mm-dd)	指定排程的開始日期。
開始時間 (hh:mm)	指定排程的開始時間。
持續時間 (hh:mm)	指定排程的持續時間。
動作	指定呼叫排程能採用的方式： **強迫啓用** - 強迫連線永遠存在。 **強迫停用** - 強迫連線永遠停止。 **啓用隨選撥接** - 指定隨選播接連線以及閒置的時間。 **停用隨選撥接** - 一旦超過閒置時間都沒有任何資料傳輸動作發生，該連線將會停止且在時間排程內都不會再啓用。
閒置逾時	若超過指定時間而沒有任何傳輸動作，系統將中斷連線。
頻率	**一次** - 此計劃的頻率只會應用一次。 **週期** - 指定一週當中哪些日子需要執行此項排程作業。

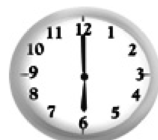
範例

假設您想要控制 PPPoE 網際網路存取連線能夠在每天的 9:00 到 18:00 都能保持開啓狀態(強迫啓用)，其他時間則中斷連線(強迫停用)。

Office Hour:

(Force On)





Mon - Sun 9:00 am to 6:00 pm

1. 確定 PPPoE 連線和**時間設定**都能正常運作。
2. 設定 PPPoE 每天早上 9:00 到下午 18:00 都保持連線狀態。
3. 設定每天晚上 18:00 到第二天早上 9:00 都是強迫停用狀態。
4. 在PPPoE網際網路存取設定檔中，指定此二個設定檔，現在PPPoE會依照時間排

程，強迫啓用與強迫停用來計畫其網際網路連線。

3.7.3 RADIUS

撥接使用者遠端認證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和說明，通常為網際網路服務供應商所廣泛應用，是用來作為驗證和授權撥接網路使用者最常見的一種方法。

建立一個 RADIUS 用戶特徵設定，可以讓路由器協助遠端撥入用戶、無線工作站以及 RADIUS 伺服器能夠共同執行驗證的動作，它可集中遠端存取驗證工作以達成網路管理。

其他應用 >> RADIUS

RADIUS 設定

☑ 啟用

伺服器 IP 位址

目標通訊埠 1812

共享密鑰

確認共享密鑰

確定 清除 取消

啓用	勾選此項以啓動 RADIUS 設定。
伺服器 **IP** 位址	輸入 RADIUS 伺服器的 IP 位址。
目標通訊埠	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值為 1812。
共享密鑰	RADIUS 伺服器和用戶共享一個用來驗證二者之間傳遞訊息的密碼，雙方都必須設定相同的共享密鑰。
確認共享密鑰	請重新輸入共享密鑰以確認。

3.7.4 UPnP

UPnP 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。

其他應用 >> UPnP

UPnP

☑ 開啟 UPnP 服務

☐ 啟用連線控制服務

☐ 啟用連線狀態服務

附註：如果您想在您的區域網路中執行 UPnP 服務，您必須勾選上面相對應的服務及UPnP設定，以便進行控制。

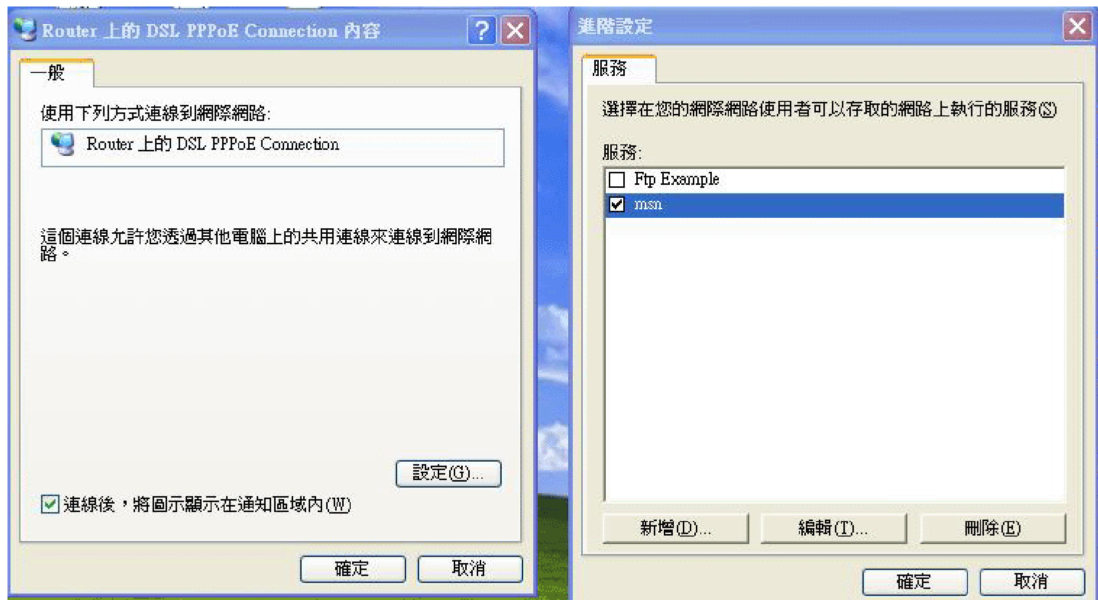
確定　清除　取消

啓用 **UPnP** 服務	您可以視情況勾選**啓用連線控制服務**或是**啓用連線狀態服務**。

在設定**啓用 UPNP 服務**後，在 Windows XP/網路連線上會出現一個 **IP Broadband Connection on Router** 圖示，連線狀態和控制狀態將可開啓使用，NAT Traversal of UPnP 可啓動應用程式中的多媒體特徵，必須手動設定通訊埠對應或是使用其他類似的方法來設定，以下顯示此項功能的範例圖形。



在路由器上的 UPnP 功能，允許應用程式(像是 MSN Messenger, 可察覺出 UPnP 功能)找到隱藏在 NAT 路由器之下的是什麼，此應用程式也會記住外部 IP 位址並且在路由器上設定通訊埠對應，結果這種能力可將封包自路由器的外部通訊埠傳送到應用程式所使用的內部通訊埠。



有關防火牆與 UPnP 功能之提示–

無法與防火牆軟體配合

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因為這些應用程式會擋掉某些網路通訊埠的存取能力。

安全考量

在您的網路上啓用 UPnP 功能可能會招致安全威脅，在您啓用 UPnP 功能之前您應該要小心考慮這些風險。

- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

UPnP 功能可不斷變化的新增通訊埠對應來表示一些察覺 UPnP 的應用程式，當這些應用程式不正常的運作中止時，這些對應可能無法移除。

3.7.5 網路喚醒(WOL)

區域網路上的電腦可以透過所連結的路由器來喚醒，當使用者想要從路由器喚醒指定的電腦時，使用者必須在此頁面上輸入該電腦正確的 MAC 位址。

此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啓 WOL 功能。

其他應用 >> 網路喚醒(WOL)

網路喚醒(WOL)

附註: 網路喚醒與 綁定 IP 與 MAC 位址 功能整合，只有綁定IP的電腦才能在此選擇 IP 位址來喚醒。

喚醒方式 MAC位址

IP 位址 ---

MAC 位址: : : : : : 網路喚醒!

執行結果

喚醒方式	有二種方式提供給使用者喚醒綁定 IP 的電腦，如果您選擇由 MAC 位址來喚醒的話，您必須輸入該主機正確的 MAC 位址；如果您選擇的是由 IP 位址來喚醒的話，您必須選擇正確的 IP 位址。 喚醒方式 MAC位址 / MAC位址 / IP 位址
IP 位址	已在防火牆>>綁定 IP 至 MAC 中設定完成的 IP 位址，將會出現在下拉式清單中，請自清單中選取您想要喚醒的電腦 IP。
MAC 位址	輸入被綁定之電腦的 MAC 位址。
網路喚醒	按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。

其他應用 >> 網路喚醒(WOL)

網路喚醒(WOL)

附註: 網路喚醒與 綁定 IP 與 MAC 位址 功能整合，只有綁定IP的電腦才能在此選擇 IP 位址來喚醒。

喚醒方式 MAC位址

IP 位址 ---

MAC 位址: : : : : : 網路喚醒!

執行結果

Send command to client done.

3.8 VPN 與遠端存取

VPN 是 Virtual Private Network (虛擬私有網路) 的縮寫，是一種利用公眾網路建立一個虛擬的、安全的、方便的通道。企業可透過這個安全通道讓兩個不同地方的辦公室互通內部資料或讓出差在外的辦公人員可以遠端撥入 VPN 通道擷取公司內部的資料。

下圖為 VPN 與遠端存取的主要功能項目：



3.8.1 遠端存取控制

這個設定可以啟動必要的 VPN 服務，如果您想要在區域網路中執行 VPN 伺服器功能，您一定要適度關閉路由器的 VPN 服務，讓 VPN 通道暢通，並關閉類似 DMZ 或是開放埠等 NAT 設定。

VPN與遠端存取 >> 遠端存取控制設定

遠端存取控制設定

- [x] 啟用 PPTP VPN 服務
- [x] 啟用 IPSec VPN 服務
- [x] 啟用 L2TP VPN 服務
- [ ] 啟用ISDN撥入

附註：如果您想在您的區域網路中架設VPN伺服器，您必須適度的取消上述通訊協定及NAT設定核取方塊，以便使資料能夠通過。

確定 清除 取消

啟用 **PPTP VPN** 服務	勾選此方塊啟動經由 PPTP 通訊協定之 VPN 服務。
啟用 **IPSec VPN** 服務	勾選此方塊啟動經由 IPSec 通訊協定之 VPN 服務。
啟用 **L2TP VPN** 服務	勾選此方塊啟動經由 L2TP 通訊協定之 VPN 服務。
啟用 **ISDN** 撥入	這個功能僅適用 *i* 機型。

3.8.2 PPP 基本設定

這項功能可以應用在 PPP 相關的 VPN 連線中，諸如 PPTP、L2TP、L2TP over IPSec 等。

VPN 與遠端存取 >> PPP 基本設定

PPP 基本設定

PPP/MP 協定		指派 IP 給撥入使用者	
撥入PPP驗證	PAP 或 CHAP	起始 IP 位址	192.168.1.200
撥入 PPP 加密（MPPE）	選擇 MPPE		
雙方共同驗證（PAP）	○ 是 ⊙ 否		
使用者名稱			
密碼			

確定

撥入 PPP 驗證　選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。

PAP 或 CHAP　選擇此項目表示路由器會嘗試先以 CHAP 協定驗證撥入使用者，如果撥入使用者沒有支援此項協定，系統會改用 PAP 協定來驗證使用者。

撥入 PPP 加密(MPPE)　此選項代表 MPPE 加密方式是由路由器針對遠端撥入使用者選擇性採用的方法，如果遠端撥入使用者沒有支援 MPPE 加密演算式，路由器將會傳送無 MPPE 加密封包出去，否則 MPPE 加密將直接用於資料加密處理。

選擇 MPPE
選擇 MPPE
MPPE（40/128 bit）
MPPE (128 bit)

MPPE (40/128bit) - 選擇此項目可以強迫路由器利用 MPPE 加密演算式加密資料封包，此外遠端撥入使用者在使用 128-bit 之前可先使用 40-bit 執行加密動作，換言之，如果沒有支援 128-bit 加密法，系統將會自動使用 40-bit 加密方式於資料加密上。

MPPE (128bit) -此選項指出路由器將會使用 MPPE 最大值 (128 bits)來加密資料。

雙方共同驗證 (PAP)　共同驗證功能主要應用於和其他路由器或是需要雙向驗證的用戶連絡，以便取得更佳安全性能，因此當您的對點路由器需要共同驗證時，您就應該啟動此功能，並進一步指定使用者名稱和密碼。

起始 IP 位址　輸入撥入 PPP 連線的 IP 位址，您應該自本地虛擬網路中選擇一個 IP 位址，例如假設本地虛擬網路為 192.168.1.0/255.255.255.0，您可以選擇 192.168.1.200 做為起始 IP 位址，但您必須注意到前二個 IP 位址 192.168.1.200 和 192.168.1.201 乃是保留作為 ISDN 遠端撥入使用者所使用。

3.8.3 IPSec 基本設定

在 **IPSec** 基本設定中，有二種主要的配置方式。

- 第一階段：IKE 參數的協商作業包含加密、重述、Diffie-Hellman 參數值和壽命，以保護後續 IKE 交換、使用預先共同金鑰或是數位簽章(x.509)之對等驗證。協商程序起始方提出所有的原則給遠端的另一方，遠端一方嘗試尋找符合其政策之最高優先權，最後建立一個 IKE 階段 2 的安全通道。
- 第二階段：IPSec 安全協商包含驗證封包頭(AH)或是 ESP，供後續 IKE 交換和雙邊安全通道設立之檢測之用。

在 IPSec 中有二種加密方式 – 傳送與通道，傳送模式將會增加 AH/ESP 承載量並使用原始 IP 標頭來加密承載的資料，此模式只應用於本地封包上如 L2TP over IPSec，通道模式不只增加 AH/ESP 承載量也會使用新的 IP 封包頭來加密整個原始 IP 封包。

驗證封包頭(AH) 提供 VPN 雙方的 IP 封包資料驗證和整合，可以單方重述功能來達成建立訊息摘要的動作，這些摘要隨著封包傳送將放置於封包頭。接收方將會在封包上執行同樣的動作，並與所接收到的數值比較。

封裝式安全酬載(ESP)提供選擇性驗證方法，對資料機密化和防護的安全協定，可重新進行檢測。

VPN 與遠端存取 >> IPSec 基本設定

VPN IKE / IPSec 基本設定

遠端撥入使用者及動態 IP 客戶的撥入設定（LAN to LAN）。

IKE 認證方式

預先共用金鑰

確認預先共用金鑰

IPSec 安全防護方式

☑ 中級（AH）

對資料進行認證，但不會進行加密。

高級（ESP） ☑ DES ☑ 3DES ☑ AES

對資料進行認證及加密。

確定 取消

IKE 認證方式	通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。 **預先共用金鑰** - 只有支援預先共用金鑰，請指定一個金鑰作為 IKE 驗證之用。 **確認預先共用金鑰**- 確認您所輸入的共用金鑰。
IPSec 安全防護方式	**中級 (AH)** - 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 (ESP)** - 表示資料將被加密及驗證，請自下 DES、3DES 或 AES 中選取適合項目。

3.8.4 IPSec 端點辨識

不論是在 LAN-to-LAN 連線或是遠端使用者撥入連線上，如果要使用數位憑證作為對方驗證之憑據，您可以在此網頁編輯對方憑證所需的清單，如圖所示，路由器提供了 200 條數位憑證供用戶輸入相關的內容。

VPN 與遠端存取 >> IPSec 端點辨識

X509 對方 ID 帳號: | 回復出廠預設值 |

索引編號	名稱	狀態	索引編號	名稱	狀態
1.	???	×	17.	???	×
2.	???	×	18.	???	×
3.	???	×	19.	???	×
4.	???	×	20.	???	×
5.	???	×	21.	???	×
6.	???	×	22.	???	×
7.	???	×	23.	???	×
8.	???	×	24.	???	×
9.	???	×	25.	???	×
10.	???	×	26.	???	×
11.	???	×	27.	???	×
12.	???	×	28.	???	×
13.	???	×	29.	???	×
14.	???	×	30.	???	×
15.	???	×	31.	???	×
16.	???	×	32.	???	×

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> 下一頁 >>

回復出廠預設值	按此鈕清除全部設定。
索引編號	請按索引下方的號碼以進入設定頁面。
名稱	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

VPN 與遠端存取 >> IPSec 端點辨識

設定檔索引 : 1

設定檔名稱 ???

☐ 啟動這個帳號

◉ 接收任何對方 ID

○ 接受主體替代名稱

類型 IP 位址

IP

○ 接受主體名稱

國家

省份

居住地區

組織

組織單位

常用名稱

電子郵件

確定 清除 取消

設定檔名稱	請輸入此設定檔的檔名。
接收任何對方 **ID**	按此鈕可以接受任何一個電腦的連線而不理會它是誰。
接受主體替代名稱	按此鈕以決定特定之數位簽章接受符合要求的對手，本區可以是 IP 位址、網域或是電子郵件，類型下方區域方塊依據您所選的類型而有所不同，請按照實際需要填入必要資訊。
接受主體名稱	按此鈕讓特定區域的數位簽章能接受符合要求的對手，本區包含有國家、省份、居住地區、組織、單位、常用名稱及電子郵件等等。

3.8.5 遠端撥入使用者

藉由維護遠端使用者設定檔表格，您可以管理遠端存取狀況，這樣使用者可以經由驗證得以撥入或是建立 VPN 連線。您可以設定包含指定連線對點 ID、連線 ID (PPTP、IPSec Tunnel 以及 L2TP 和 L2TP over IPSec)等參數，和相關安全防護方式。

路由器提供 **200** 個存取使用者號碼予撥入用戶，此外經由內建 RADIUS 用戶端功能，您可以將帳號延伸至 RADIUS 伺服器。下圖顯示帳號總表格：

VPN 與遠端存取 >> 遠端撥入使用者

遠端存取用戶帳號: | 回復出廠預設值 |

索引編號	用戶	狀態	索引編號	用戶	狀態
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> 下一頁 >>

回復出廠預設值	按此鈕清除全部設定。
索引編號	請按索引下方的號碼以進入遠端撥入使用者之設定頁面。
用戶	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。
狀態	顯示特定撥入使用者的存取狀態，符號 V 和 X 分別代表活動中與不活動的檔案。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

VPN 與遠端存取 >> 遠端撥入使用者

索引編號 1

使用者帳號與認證	
☑ 開啟這個帳號	使用者名稱 ???
閒置逾時 300 秒	密碼
允許的撥入模式	**IKE 認證方式**
☑ ISDN	☑ 預先共用金鑰
☑ PPTP	IKE 預先共用金鑰
☑ IPSec通道	☑ 數位簽章 (X.509)
☑ 具有 IPSec 原則的 L2TP 無	無
☐ 指定遠端節點	**IPSec 安全防護方式**
遠端用戶或對方 ISDN 號碼	☑ 中級 (AH)
	高級 (ESP)
或對方 ID	☑ DES ☑ 3DES ☑ AES
	本機 ID (視需要填入)
	回撥功能
	☐ 啟動回撥功能
	☐ 指定回撥號碼
	回撥號碼
	☑ 啟動剩餘回撥時間控制
	剩餘回撥時間 30 分

確定 清除 取消

開啓這個帳號	勾選此方塊以啓用此功能。 **閒置逾時** - 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時爲 300 秒。
ISDN	可建立 ISDN 撥入連線至伺服器，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。您可進一步設定回撥功能，此選項僅作用於 *i* 機型。
PPTP	爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。
IPSec 通道	允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。
具有 **IPSec** 原則的 **L2TP**	爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： **無** - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 **建議選填** -如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入 VPN 連線會成爲一種完全的 L2TP 連線。 **必須** - 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。
指定遠端節點	**勾選** - 您可以指定遠端撥入使用者或是對點 ID (應用於 IKE 主動模式中)的 IP 位址。

	不勾選 - 表示您所選擇的連線類型，將會應用**一般設定**中所設定的驗證方式和安全防護方式。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
IKE 驗證方式	**預先共同金鑰-** 勾選此方塊啓用此功能並輸入 1-63 文字做為預先共同金鑰。 **數位簽章 (X.509) –**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容。
安全防護方式	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。請勾選中級或是高級設定作為安全防護方式。 **中級 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級-Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID -**指定一個本地 ID 以便作為 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。
回撥功能	回撥功能針對 ISDN 撥入用戶提供回撥服務，電信公司將向路由器所有人索取連線費用。(針對 *i* 系列) **啓動回撥功能** – 啓動回撥功能。 **指定回撥號碼** -此選項可提供額外的安全防護，一旦啓動了，路由器只會回撥給指定的回撥號碼。 **啓動剩餘回撥時間控制** – 回撥功能的預設值是有時間限制的，一旦回撥時間超時，回撥機制將自動關閉。 **剩餘回撥時間 (單位:分鐘)** –指定撥入用戶的剩餘回撥時間。

3.8.6 設定 LAN to LAN

您可以透過維護連線檔案的表格來管理 LAN-to-LAN 連線，您可設定包含指定連線方向(撥進或是撥出)的參數、連線對方的 ID、連線型態(VPN 含 PPTP, IPSec Tunnel 和 L2TP 或是其他)以及相關的安全防護方法等等。

路由器提供 **200** 個設定檔，也就是說同時可以支援 **200** 個 VPN 頻道，下圖顯示設定檔案的清單表格。

VPN 與遠端存取 >> LAN to LAN

LAN-to-LAN 設定檔: | 回復出廠預設值 |

索引編號	名稱	狀態	索引編號	名稱	狀態
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> 下一頁 >>

回復出廠預設值	按此鈕清除全部設定。
索引編號	請按索引下方的號碼以進入設定頁面。
名稱	意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。
狀態	表示個別檔案的狀態，符號 V 和 X 分別代表使用中與未使用的檔案。

請按索引連結以編輯個別設定檔，按下後可看到如下的頁面，每個 LAN-to-LAN 檔案包含有四個子群組，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

由於網頁太長，我們將之切成數個段落來說明。

VPN 與遠端存取 >> LAN to LAN

設定檔索引 : 1

1. 一般設定

設定檔名稱 ???
啟用此設定檔
VPN 連線經由介面: WAN1 優先

撥號方向 雙向 撥出 撥入
永遠連線
閒置逾時 300 秒
啟用 PING 以維持連線
指定 IP 位址

2. 撥出設定

我撥出的伺服器類型
ISDN
PPTP
IPSec
具有 IPSec 原則的 L2TP 無

ISDN 撥接號碼或
對方 VPN 所需之伺服器 IP 或域名.
(例如 5551234, draytek.com 或 123.45.67.89)

連接類型 64k bps
使用者名稱 ???
密碼
PPP 驗證 PAP/CHAP
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰
數位簽章(X.509)
無

IPSec 安全防護方式
中級(AH)
高級(ESP) DES 無驗證
進階

索引號碼(1-15) 於 排程 設定:

回撥功能 (CBCP)
所需回撥的遠端
提供 ISDN 號碼予遠端

設定檔名稱　　針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。

啟用此設定檔　　按此方塊啟用此設定檔。

VPN 連線經由介面　　使用下拉式選項選擇適合的 WAN 介面，此設定僅適合撥出時使用。

WAN1 優先
WAN1 優先
僅用 WAN1
WAN2 優先
僅用 WAN2

WAN1 優先 - 連線時，路由器會將 WAN1 視為 VPN 連線的首要選擇，如果 WAN1 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN1 - 連線時，路由器會將 WAN1 視為 VPN 連線的唯一選擇。

WAN2 優先 - 連線時，路由器會將 WAN2 視為 VPN 連線的首要選擇，如果 WAN2 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN2 - 連線時，路由器會將 WAN2 視為 VPN 連線的唯一選擇。

撥號方向　　針對此 LAN-to-LAN 連線，請指定允許的撥號方向。

雙向 – 發話方/接話方

	撥出 - 發話方 **撥入** - 接話方
永遠連線或閒置逾時	**永遠連線** – 勾選此方塊讓路由器永遠保持 VPN 連線。 **閒置逾時** - 預設值為 300 秒，若連線閒置時間超過此數值，路由器將自動中斷連線。
啓用 **PING** 以維持連線	此功能可協助路由器決定 IPSec VPN 連線狀態，對不正常的 IPSec VPN 通道中斷尤其有用。詳細內容請參考下面的註解，請勾選此方塊啓動 PING 封包傳輸至指定的 IP 位址。
指定 **IP** 位址	輸入位於 VPN 通道另一邊的遠端主機的虛擬 IP 位址。

> **註解：啓用 PING 以維持連線**用來管理不正常的 IPSec VPN 連線中斷，提供一個 VPN 連線狀態供路由器判斷是否需要重撥。
>
> 正常而言，如果 VPN 任何一方想要中斷連線，那麼就必須依照封包交換程序通知對方。不過如果另一方在未通知的情況下中斷連線，Vigor 路由器將無從得知此項訊息，為了解決這樣的困境，藉著不斷傳送 PING 封包至遠端主機的方式，路由器就可以知道此項 VPN 通道有無實際運作，這是一種獨立的 DPD (無效對方檢測)。

PPTP	為伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。
IPSec	為伺服器建立一個透過網際網路的 IPSec VPN 連線。
具有 **IPSec** 原則的 **L2TP**	為伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： **無** - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 **建議選填** -如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成為一種完全的 L2TP 連線。 **一定要有** - 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
PPP 認證	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。PAP/CHAP 是最平常的選項。
VJ 壓縮	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作為 TCP/IP 協定標頭壓縮之用，通常設定選擇**開啓**以改善頻寬利用的狀況。

IKE 驗證方式

預先共用金鑰-選擇此項目啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。

數位簽章 (X.509) – 請按此鈕並自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辯識**中所預先定義的設定檔。

IPSec 安全防護方式

對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。

中級 (AH) 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。

高級 (ESP-Encapsulating Security Payload) 表示資料將被加密及驗證，請自下拉式清單中選取適合項目：

DES 無驗證 - 使用 DES 加密演算式，但不採用任何驗證計畫。

DES 有驗證 - 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

3DES 無驗證 - 使用三重 DES 加密演算式，但不採用任何驗證計畫。

3DES 有驗證 -使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

AES 無驗證 - 使用 AES 加密演算式，但不採用任何驗證計畫。

AES 有驗證 -使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

進階

指定模式、建議和 IKE 階段金鑰有效時間等設定，可按**進階**按鈕進入進階設定，視窗顯示如下：

http://192.168.1.1 - IKE 進階設定 - Microsoft Internet Explorer

IKE 進階設定

IKE 階段 1 模式 — Main 模式 / Aggressive 模式
IKE 階段 1 建議 — DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2
IKE 階段 2 建議 — HMAC_SHA1/HMAC_MD5
IKE 階段 1 金鑰有效時間 — 28800 (900~86400)
IKE 階段 2 金鑰有效時間 — 3600 (600~86400)
Perfect Foward Secret(PFS) — 停用 / 啟用
本機 ID

確定 關閉

完成 網際網路

IKE 階段 1 模式 – 選擇 **Main 模式**或是 **Aggressive 模式**。比起 **Aggressive 模式**，**Main 模式**顯得更加安全，因爲在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值爲 **Main 模式**。

IKE 階段 1 建議 - 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對 **Main 模式**來說有九種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。

IKE 階段 2 建議 - 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對

二種模式來說有 3 種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。

IKE 階段 1 金鑰有效時間- 考慮到安全之故，使用者必須訂定有效時間，預設值為 28800 秒，您可以在 900 與 86400 秒之間指定所需的時間值。

IKE 階段 2 金鑰有效時間- 考慮到安全之故，使用者必須訂定有效時間，預設值為 3600 秒，您可以在 900 與 86400 秒之間指定所需的時間值。

PFS – 停用或是啟用此特殊功能。

本機 ID – 在 **Aggressive** 模式中，當鑑定遠端 VPN 伺服器身分時，本機 ID 代表 IP 位址，ID 長度限制於 47 個字元。

回撥功能
(適用於 *i* 機型)

回撥功能針對 ISDN 撥入用戶提供回撥服務作為 PPP 的一部份，電信公司將向路由器所有人索取連線費用。

所需回撥的遠端 - 勾選此項可讓路由器要求遠端用戶稍後回撥。

提供 ISDN 號碼予遠端 -遠端用戶需要路由器回撥時，需有本地 ISDN 號碼，請勾選此項，允許路由器傳送 ISDN 號碼給與遠端路由器，此項功能僅對 *i* 機型有作用。

3. 撥入設定

允許的撥入模式
☑ ISDN
☑ PPTP
☑ IPSec
☑ 具有 IPSec 原則的 L2TP 無

☐ Specify ISDN CLID 或 遠端 VPN 閘道
對方 ISDN 號碼或對方 VPN 伺服器 IP
或對方 ID

使用者名稱 ???
密碼
VJ 壓縮 ⦿ 開啟 ○ 關閉

IKE 驗證方式
☑ 預先共用金鑰
IKE 預先共用金鑰
☐ 數位簽章(X.509)
無

IPSec 安全防護方式
☑ 中級 (AH)
高級 (ESP)
☑ DES ☑ 3DES ☑ AES

回撥功能 (CBCP)
☐ 啟用回撥功能
☐ 使用下列號碼回撥
回撥號碼
剩餘回撥時間 0 分(s)

4. TCP/IP網路設定

我的 WAN IP 0.0.0.0
遠端閘道 IP 0.0.0.0
遠端網路 IP 0.0.0.0
遠端網路遮罩 255.255.255.0
更多

RIP 方向 停用
RIP 版本 版本 2
第一子網段到遠端網路要做 路由
☐ 指定此 VPN 通道為預設路由

確定 清除 取消

允許的撥入類型

以不同類型來決定撥入連線。

ISDN

允許遠端 ISDN 撥入連線。您可進一步設定稍後的回撥功能，請設定遠端撥入用戶的使用者名稱和密碼。此項功能僅對 *i* 機型有作用。

PPTP	允許遠端撥入用戶透過網際網路達成 PPTP VPN 連線，請設定遠端撥入用戶的使用者名稱和密碼。
IPSec	允許遠端撥入用戶透過網際網觸發 IPSec VPN 連線。
具有 **IPSec** 原則的 **L2TP**	允許遠端撥入用戶透過網際網路製造 L2TP VPN 連線，您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： 無 - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP 可以在完全 L2TP 連線中檢視內容。 建議選填-如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成爲一種完全的 L2TP 連線。 必須 - 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。
指定 **ISDN CLID** 或 遠端 **VPN** 閘道	您可勾選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。 若您選擇 ISDN 類型，請於此輸入對方的 ISDN 號碼， (適用於 *i* 機型)。 此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
VJ 壓縮	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作爲 TCP/IP 協定標頭壓縮之用。
IKE 驗證方式	當您指定遠端節點的 IP 位址時，IKE 驗證可套用在 IPSec 通道和含 IPSec 原則之 L2TP 上。不過，不管有沒有指定遠端節點的 IP 位址予 IPSec 通道使用，您仍然可以設定數位簽章(X.509)。 **預先共同金鑰-** 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。 **數位簽章 (X.509) –**勾選此方塊啓用此功能並自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辯識**中所預先定義的設定檔。
IPSec 安全防護方式	當您指定遠端模式時，對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。 **中級 (AH)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 (ESP-Encapsulating Security Payload)-** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目。
回撥功能	回撥功能針對 ISDN 撥入用戶(此項功能僅對 *i* 機型有作用)提供回撥服務，電信公司將向路由器所有人索取連線費用。 **啓用回撥功能** - 勾選此項可讓路由器要求遠端用戶稍後回撥。

使用下列號碼回撥 – 勾選此項以便使用下列設定的號碼回撥。

回撥號碼 – 輸入回撥號碼。

剩餘回撥時間 - 指定撥入用戶的剩餘回撥時間，每次回撥連線，時間將自動降低，預設值 0 表示回撥期間沒有時間限制。

我的 WAN IP	本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將從遠端路由器取得您所指定的 IP 位址，請在此輸入 IP 位址。此一位址適用於本機為 VPN client (dial-out) 端時。
遠端閘道 IP	本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將發予對方的 IP 位址，請在此輸入發予對方之 IP 位址。此一位址適用於本機為 VPN Server (dial-in) 端時。
遠端網路 IP/遠端網路遮罩	新增一個靜態路由以便透過網際網路，引導遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。對 IPSec 而言，這項設定是第二階段快速模式的目的用戶端之身分。
更多	新增一個靜態路由，並藉由網際網路引導更多的遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。通常在您發現遠端 VPN 路由器有數個子網路存在時，您會使用此按鈕設定更多的路由。
RIP 方向	此選項指定 RIP (路由資訊協定) 封包的方向，您可以啟用也可以停用 RIP 方向，於此，我們提供您四種選擇：TX/RX 二者均有、TX、RX 以及停用。
第一子網段到遠端網路要做	若對方網路只提供單一 IP 撥入，請在此選擇 **NAT**，否則請選擇**路由**。 路由 路由 NAT
指定此 VPN 通道為預設路由	勾選此方塊指定此 VPN 通道為預設路由，注意此設定只有在一個 WAN 介面啟用時有效，若是二個 WAN 介面皆啟用，此功能即無法使用。

3.8.7 連線管理

您可以查看全部 VPN 連線的總結清單，您可中斷任何一個 VPN 連線，只要輕輕按下中斷按鈕即可。您也可以使用撥出工具並按**撥號**按鈕主動撥出任何的電話。

VPN 與遠端存取 >> 連線管理

撥出工具　　更新間隔秒數: 10　更新頁面

撥號

VPN 連線狀態

目前所在頁面 1　　頁面編號　前進該頁　>>

VPN	類型	遠端 IP	虛擬網路	傳送封包數	傳送速率	接收封包數	接收速率	運作時間

xxxxxxxx:資料已加密。
xxxxxxxx:資料未加密。

撥號	按此鈕執行撥號功能。
更新間隔秒數	選擇重新顯示狀態的間隔秒數，有 5、10、30 秒等三種選擇。
更新頁面	按此鈕以重新顯示整個連線狀態。

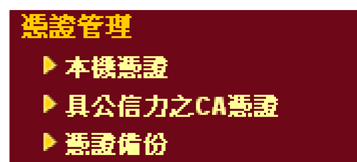
3.9 憑證管理

數位憑證就像是一個電子 ID，此 ID 可以由憑證授權中心註冊取得。它包含有您的名字、序號、到期日、憑證授權的數位簽章，這樣一來，接收者可以確認該憑證是否是真實的。本路由器支援遵守標準 X.509 的數位憑證。

任何想要使用數位憑證的人都應該先有 CA 伺服器註冊的憑證，此憑證也可從其他具公信力的 CA 伺服器取得，如此還可以驗證其他從公信力的 CA 伺服器取得憑證的另一方。

此處您可以管理產生本機的數位憑證，並設定具公信力之 CA 憑證，使用憑證前，請記得調整路由器的時間，這樣才可取得正確的憑證有效期。

下圖顯示憑證管理的功能項目：



3.9.1 本機憑證

這個網頁可讓您設定本機憑證的基本資料。

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主體	狀態	編輯
本機	---	---	檢視 刪除

產生 匯入 頁面更新

X509 本機憑證

產生　　　按此鈕以開啓**產生憑證需求**視窗。

憑證管理 >> 本機憑證

產生憑證需求

主體替代名稱	
類型	IP 位址
IP	
主體名稱	
國家	
省份	
居住地區	
組織	
組織單位	
常用名稱	
電子郵件	
金鑰類型	RSA
金鑰大小	1024 Bit

產生

輸入全部的資訊(如 AN IP 位址，網域名稱，電子郵件，主體名稱的相關資料)，然後再按一次**產生**按鈕。所有的資料請以英文輸入文。

匯入　　　按此鈕以匯入儲存的檔案作爲憑證資訊。

憑證管理 >> 本機憑證

匯入 X509 本機憑證

選擇本機憑證檔案

瀏覽...

按 匯入 上傳本機憑證。

匯入　取消

頁面更新　　　按此鈕以更新資訊。

檢視　　　按此鈕以檢視憑證詳細的設定。

在按下**產生**按鈕之後，產生後的資訊將會顯示在視窗上，見下圖：

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主題	狀態	編輯
本機	/C=TW/O=Draytek/emailAddress...	Requesting	檢視 刪除

產生　匯入　頁面更新

X509 本機憑證設定需求


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYXl0ZWsxIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdHblo1kt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7evl87twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQAuSBRUGt4WlhH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO8Jx0I45560xCZ/NlGh9VQ9Il
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```

3.9.2 具公信力之 CA 憑證

具公信力之 CA 憑證列出三組具公信力之 CA 憑證表。

憑證管理 >> 具公信力之 CA 憑證

X509 具公信力之 CA 憑證設定

名稱	主體	狀態	編輯
Trusted CA-1	---	---	檢視 刪除
Trusted CA-2	---	---	檢視 刪除
Trusted CA-3	---	---	檢視 刪除

匯入 更新頁面

若要輸入事先儲存的具公信力之 CA 憑證，請按**匯入**鈕開啓如下的視窗，並使用**瀏覽…**找到儲存的文字檔案，接著按下**匯入**鈕，您所要匯入的檔案將會列在視窗上，再按一次**匯入**鈕即可使用預先儲存的檔案。

憑證管理 >> 具公信力之CA憑證

匯入 X509 具公信力之CA憑證

選擇具公信力之CA憑證檔案

瀏覽...

按一下 匯入 上傳憑證

匯入 取消

如要檢視每個具公信力之 CA 憑證，請按**檢視**按鈕開啓憑證的詳細資訊視窗，如果您想要刪除 CA 憑證，選擇該憑證並按下**刪除**按鈕，所有相關的憑證資訊即可刪除。

http://192.168.1.1 - 憑證資訊 - Microsoft Internet Explorer

憑證詳細資訊

憑證名稱:	Trusted CA-1
發行者:	
主題:	
主題替代名稱:	
有效期自:	
有效期至:	

關閉

3.9.3 憑證備份

路由器的本機憑證與具公信力之 CA 憑證可以儲存為一個檔案，請按下述畫面的備份按鈕來儲存，如果您想要設定加密的密碼，請在**加密密碼**與**確認密碼**二欄中輸入所需的字元。

此外您隨時可以使用**還原**按鈕取回這二項設定套用至路由器上。

憑證管理 >> 憑證備份

備份/還原憑證

備份

加密密碼

確認密碼:

按 備份 下載憑證至本機電腦並存成檔案。

還原

選擇備份檔案以還原。

瀏覽...

解密密碼

按 還原 上傳檔案。

3.10 無線區域網路設定

注意 ： 本節所提供的資訊僅針對 G 系列機型。

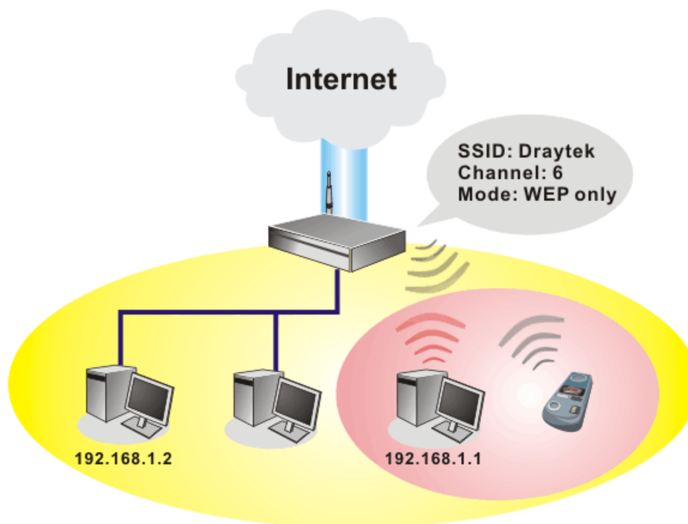
3.10.1 基本觀念

在最近幾年無線通訊的市場有了極大的成長，無線技術線在到達了或說是有能力到達地球表面上的每一個點，數以百萬的人們每天透過無線通訊產品彼此交換資訊，Vigor G 系列路由器，又稱為 Vigor 無線路由器，被設計成為一個適合小型辦公室/家庭需要的路由器，擁有最大的彈性與效率，任何一個被授權的人，都可以攜帶內建的無線區域網路用戶端 PDA 或是筆記型電腦，進入會議室開會，因而不需擺放一堆亂七八糟的纜線或是到處鑽孔以便連線。無線區域網路機動性高，因此無線區域網路使用者可以同時存取所有區域網路中的工具，以及遨遊網際網路，好比是以有線網路連接的一樣。

Vigor 無線路由器皆配有與標準 IEEE 802.11g 通訊協定相容之無線區域網路介面，為了進一步提高其效能，Vigor 路由器也承載了進階無線技術 Super G TM 以便將速率提升至 108 Mbps*，因此在最後您可以非常順利的享受流暢的音樂與影像。

注意：*資料的實際總處理能力會依照網路條件和環境因素而改變，如網路流量、網路費用以及建造材料。

在無線網路的基礎建設模式(Infrastructure Mode)中，Vigor 無線路由器扮演著無線網路基地台(AP)的角色，可連接很多的無線用戶端或是無線用戶站(STA)，所有的用戶站透過路由器，都可分享相同的網際網路連線。**基本設定**可讓您針對無線網路所需的訊息包含 SSID、頻道等項目做基本的配置。



安全防護概要

即時硬體加密: Vigor 路由器配有 AES 加密引擎，因此可以採用最高級的保護措施，在不影響使用者的習慣之下，對資料達成保護效果。

完整的安全性標準選項: 為了確保無線通訊的安全性與私密性，提供數種市場上常見的無線安全標準。

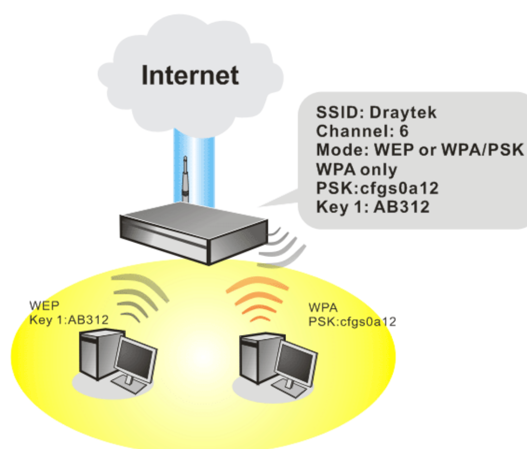
有線對應隱私權(Wired Equivalent Privacy, WEP)是一種傳統的方法，使用 64-bit 或是 128-bit 金鑰透過無線收發裝置來加密每個資料訊框。通常無線基地台會事先配置一組含四個金鑰的設定，然後使用其中一個金鑰與每個無線用戶端通訊聯絡。

Wi-Fi 保護存取協定(Wi-Fi Protected Access, WPA)是工業上最佔優勢的安全機制，可分成二大類：WPA-personal 或稱為 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱為 WPA/802.1x。

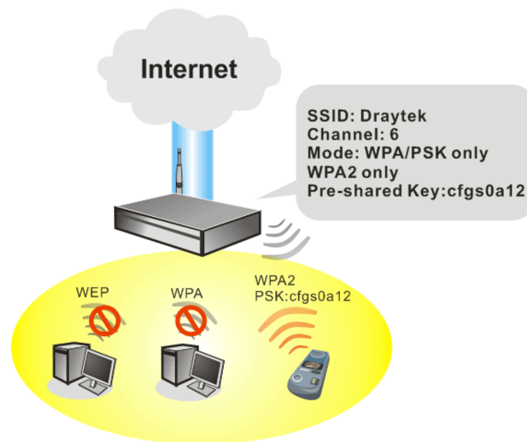
在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作為安全連線之用。您應該按照所需來選擇適當的安全機制，不論您選擇哪一種安全防護措施，它們都可以全方位的加強您無線網路上之資料保護以及/或是機密性。Vigor 無線路由器是相當具有彈性的，且能同時以 WEP 和 WPA 支援多種安全連線。

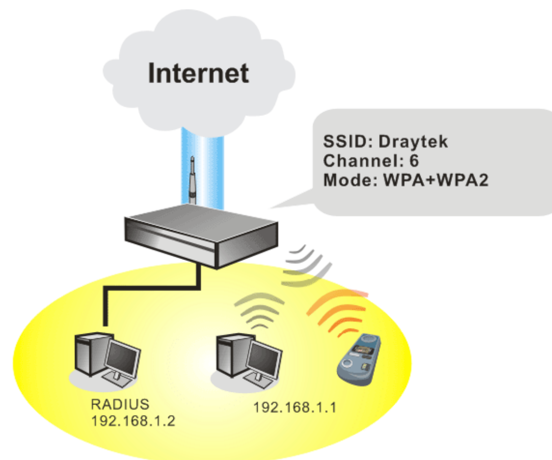
範例 1



範例2



範例3



分隔無線與有線區域網路 - 無線區域網路隔離可使您自有線區域網路中,分隔出無線區域網路以便隔離或是限制存取。隔離代表著雙方彼此都無法存取對方的資料，欲詳細說明商業用途之範例，您可以為訪客設定一個無線區域網路，讓他們只能連接到網際網路而不必擔心洩露機密資訊。更彈性的作法是，您可以新增 MAC 位址的過濾器來區隔有線網路之單一使用者的存取行為。

管理無線用戶端 - 無線用戶端列表顯示無線網路中全部的無線用戶端以及連接狀態。

以下為**無線區域網路**下的功能項目：

無線區域網路
- 基本設定
- 安全性設定
- 連線控制
- WDS
- 搜尋無線基地台
- 無線用戶端列表
- 站台流量控制

3.10.2 基本設定

按下一般設定連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：

無線區域網路 >> 基本設定

基本設定 (IEEE 802.11)

☑ 啟用

模式 綜合(11b 和 11g)

索引(1-15) 於 排程 設定: , , ,

SSID default

頻道 頻道 6, 2437MHz

附註 如果啟動 SuperG 模式，頻道將固定在 6。

☐ 隱藏 SSID

☐ 長封包標頭

隱藏 SSID：不讓 SSID 被掃描到

長封包標頭：和某些 802.11b 設備連線時需要(低效率)。

確定 取消

啓用 勾選此方塊啓動無線功能。

模式 請選擇一個適當的無線模式。

綜合(11b 和 11g+SuperG) – 無線通訊同時支援協定 IEEE802.11b、IEEE802.11g 和 **SuperG)**。

綜合(11b 和 11g) – 無線通訊同時支援二種協定 IEEE802.11b 與 IEEE802.11g。

SuperG -無線通訊僅支援 SuperG。

11g - 無線通訊僅支援 IEEE802.11g。

11b -無線通訊僅支援 IEEE802.11b。

模式 綜合(11b 和 11g)

綜合 (11b,11g 和 SuperG)
綜合(11b 和 11g)
SuperG
11g
11b

索引(1-15) 設定無線區域網路在特定的時間間隔中運作。您可以從**應用**的**排程設定**頁面上，自 15 個排程中選擇 4 個，本區預設值是空白的，表示無線功能是永遠可以運作的狀態。

SSID 預設的 SSID 值爲 **default**，建議您變更爲另一個特殊名稱。它是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。

頻道	無線區域網路的通道頻率，預設頻道是 6，如果選定的頻道受到嚴重的干擾的話，您可自行切換為其他頻道。 頻道 頻道 6, 2437MHz 頻道 1, 2412MHz 頻道 2, 2417MHz 頻道 3, 2422MHz 頻道 4, 2427MHz 頻道 5, 2432MHz 頻道 6, 2437MHz 頻道 7, 2442MHz 頻道 8, 2447MHz 頻道 9, 2452MHz 頻道 10, 2457MHz 頻道 11, 2462MHz 頻道 12, 2467MHz 頻道 13, 2472MHz
隱藏 SSID	勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。
長封包標頭	此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。

3.10.3 安全性設定

擇安全性設定後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。

無線區域網路 >> 安全性設定

安全性設定

模式 WEP 或 WPA/PSK

設定 RADIUS 伺服器 若您已啟用 802.1x 功能

WPA:

類型 綜合(WPA+WPA2) WPA2

預先共用金鑰 (PSK) *************

輸入 8~63 個 ASCII字元或以 "0x" 為首後接 64 個十六進位字元，例如 "cfgs01a2..." 或 "0x655abcd...."。

WEP:

加密模式 64-Bit

使用 WEP 金鑰

金鑰 1 *************

金鑰 2 *************

金鑰 3 *************

金鑰4 *************

就 64-bit WEP 金鑰而言

輸入 5 個 ASCII 字元或開頭為 "0x" 的 10 個十六進位數字，如 "AB312" 或 "0x4142333132"。

就 128-bit WEP 金鑰而言

輸入 13 個 ASCII 字元或開頭為 "0x" 的 26 個十六進位數字，如 "0123456789abc" 或 "0x30313233343536373839414243"。

確定 取消

模式

此一設定有數種模式可供您選擇。

模式 停用

停用
WEP
WEP/802.1x
WEP 或 WPA/PSK
WEP/802.1x 或 WPA/802.1x
WPA/PSK
WPA/802.1x

停用 - 關閉加密機制。

WEP - 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。

WEP/802.1x - 接受以 802.1X 驗證方式來驗證的 WEP 用戶。

WEP 或 WPA/PSK -接受以合法金鑰的內容來驗證的 WEP 和 WPA 用戶。

WEP/802.1x 或 WPA/802.1x -接受以 802.1X 驗證方法來驗證的 WEP 或是 WPA 用戶。

WPA/PSK -接受 WPA 用戶，請在 PSK 中輸入加密金鑰。

WPA/802.1x Only -接受以 802.1X 驗證方式驗証的 WPA 用戶。

注意: 如果您選擇了 WEP/802.1x 或 WPA/802.1x, WEP/802.1x 或者是 WPA/802.1x 模式,您還必需同時設定 RADIUS 伺服器。

WPA

WPA 可藉由金鑰加密每個來自無線網路的訊框,可在本區手動輸入 PSK,或是藉由 802.1X 驗證方式來自動加密。

類型 – 選擇綜合 (WPA+WPA2) 或 WPA2。

預先共用金鑰 (PSK) - 輸入 **8~63** 個 ASCII 字元,像是 012345678(或是 64 個 16 進位數字,以 0x 開頭,如 0x321253abcde...)。

WEP

64-Bit - 針對 64 位元的 WEP 金鑰,請輸入 5 個 ASCII 字元,像是 12345(或是 10 個 16 進位數字,以 0x 開頭,如 0x4142434445)。

128-Bit - 針對 128 位元的 WEP 金鑰,請輸入 13 個 ASCII 字元,像是 ABCDEFGHIJKLM(或是 26 個 16 進位數字,以 0x 開頭,如 0x4142434445)。

加密模式: 64-Bit

64-Bit
128-Bit

所有的無線裝置都必須支援相同的 WEP 加密位元大小,並擁有相同的金鑰。這裡可以輸入四組金鑰,但一次只能選擇一組號碼來使用,這些金鑰可以 ASCII 文字或是 16 進位字元來輸入。請點選您想使用的金鑰組別。

3.10.4 連線控制

為了增加額外的無線存取安全性，連線控制頁面可讓您透過無線區域網路的用戶 MAC 位址來限制網路存取動作。只有設定有效的 MAC 位址得以存取無線區域網路介面，請選**連線控制**連結，開啓新的網頁，如同下圖所示，您即可在此頁面上編輯用戶端的 MAC 位址達到控制其存取權的目的。

無線區域網路 >> 連線控制

連線控制 | 回復出廠預設值 |

☑ 啟用連線控制

規則： 啟用 MAC 位址過濾程式

MAC 位址過濾

索引 特性 MAC 位址

客戶端的 MAC 位址： : : : : :

特性：

☐ s: 將此無線站台和有線網路隔離

新增 刪除 編輯 取消

確定 全部清除

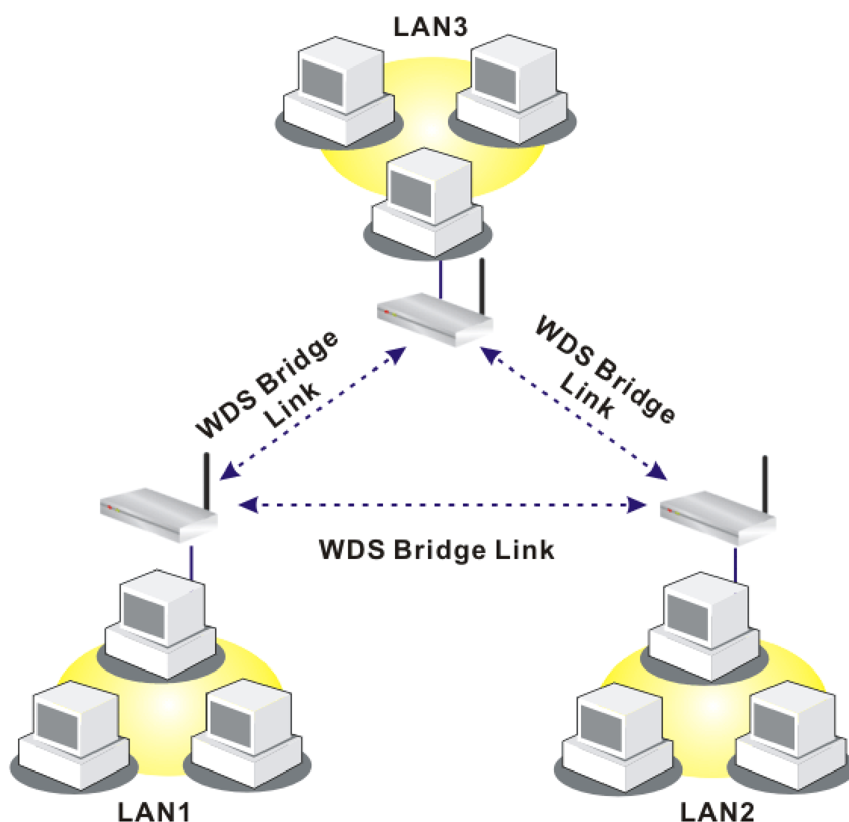
啓用連線控制	勾選此項以啓動 MAC 位址存取控制作用。
規則	選擇一項規則，請挑選**啓用 MAC 位址過濾程式**以便在下方手動輸入其他用戶的 MAC 位址；挑選**隔離無線網路和有線網路**可以 MAC 位址清單爲基礎，自區域網路中隔開所有的無線網路用戶站。 規則： 啟用MAC位址過濾程式 啟用MAC位址過濾程式 隔離無線網路和有線網路
MAC 位址過濾	顯示之前編輯的全部 MAC 位址。 **客戶端的 MAC 位址** - 請手動輸入無線用戶端的 MAC 位址。
特性	**s** -勾選此項以便隔離無線用戶端之無線連線。
新增	新增新的 MAC 位址於清單上。
刪除	刪除清單中選定的 MAC 位址。
編輯	編輯清單中選定的 MAC 位址。
取消	放棄連線控制設定。
確定	按此鈕儲存連線控制清單。
全部清除	按此鈕儲存連線控制清單。

3.10.5 WDS

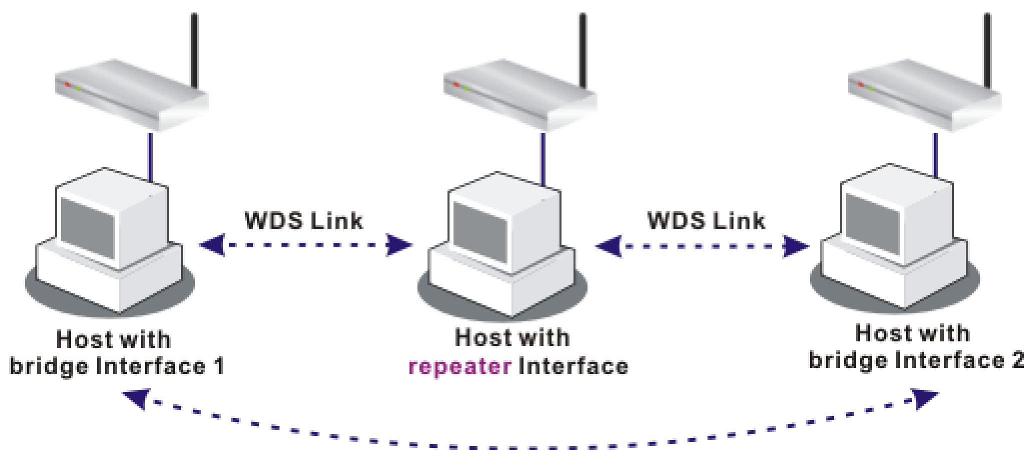
WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

- 提供二個區域網路間空中交流的橋樑
- 延長無線區域網路的涵蓋範圍

迎合以上的需要，路由器可應用二種 WDS 模式，一爲**橋接**一爲**中繼**，下圖顯示 WDS 橋接介面的功能：

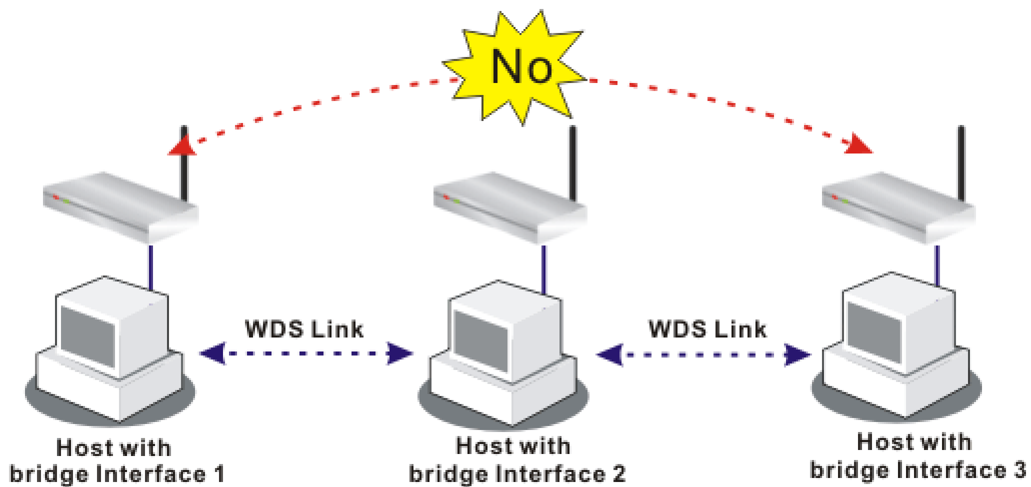


WDS-中繼模式的應用則描繪如下：



二種模式的主要不同點在於：**中繼**模式下，從一端 AP 過來的封包可以透過 WDS 連結再另一個 AP 上重複產生，WDS 連結傳送過來的封包只能轉送至本機有線或無線的主機。換言之，只有此模式能完成 WDS 到 WDS 封包轉送的工作

在下面這個例子當中，連接至橋接介面 1 或 3 的主機可以透過 WDS 連結與橋接介面 2 相連。不過連接至橋接 1 的主機無法透過橋接介面 2 與橋接介面 3 的主機相通。



按無線區域網路中的 **WDS** 功能以出現如下畫面：

無線區域網路 >> WDS 設定

WDS 設定 | 回復出廠預設值 |

模式: 橋接

安全性:
停用 WEP 預先共用金鑰 (PSK)

WEP:
使用相同WEP金鑰設定於 安全性設定.
加密模式 : 64-bit
金鑰索引 : 1
若安全模式設定不是 "WEP"，則金鑰索引為鎖定狀態且不可變更。
金鑰 : *************
金鑰格式應和另一支相同 安全性設定.

預先共用金鑰 (PSK)
類型 : TKIP
金鑰 : *************
輸入 8到63個 ASCII字元或以"0x"開頭的64個十六進位字元.例如:"cfgs01a2..." 或 "0x655abcd...."。

橋接
啟用 對方的 MAC 位址
附註:為提升效率，將中斷未使用的連線。

中繼
啟用 對方的 MAC 位址

無線基地台功能:
啟用 停用

狀態:
送出 "Hello" 訊息給對方
連線狀態
附註:此功能只有當對方也支援該功能時才有效。

確定 清除 取消

模式　　選擇 WDS 設定模式，停用將無法啓用任何 WDS 設定；**橋接**模式乃是設計用來符合第一種實際之應用；**中繼**模式則是設計用來符合第二種實際之應用。

模式: 橋接
停用
橋接
中繼

安全性	有三種安全性類型可選擇，停用、WEP 和預設共用金鑰。您在此處所選擇的設定將會使得 WEP 或是預設共用金鑰有效或是無效。請自三種中挑選出一種。
WEP	勾選此方塊使用安全性設定頁面中同樣的金鑰。如果您並未在安全性設定頁面中設定任何的金鑰，此方塊將暫時無法使用。 加密模式 – 如果您勾選使用相同 WEP 金鑰於…，您不需要選擇 64-bit 或 128-bit 做爲加密模式；如果您並未勾選該方塊，您就可在本頁設定 WEP 金鑰。 金鑰索引 -完成適當的加密模式後，請選擇您想要使用的金鑰相對索引號碼。 金鑰 -輸入金鑰的內容。
預設共用金鑰	輸入開頭爲“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。
橋接	如果您選擇橋接做爲通訊模式,請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入六個對方 MAC 位址。停用不使用的連結可以取得較好的執行效果，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選啓用方塊。
中繼	如果您選擇中繼做爲通訊模式,請在此區輸入對方的 MAC 位址,本頁可讓您一次輸入二個對方 MAC 位址。同樣的，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選啓用方塊。
無線基地台功能	按啓用讓路由器提供無線基地台的服務；按停用取消此功能。
狀態	允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。

3.10.6 搜尋無線基地台

路由器可以掃描全部的頻道以及發現鄰近地區運作中的無線基地台，基於掃描的結果，使用者將會知道哪個頻道是可用的，此外它也可以用來發現 WDS 連結中的無線基地台，注意在掃描過程中(約 5 秒)，任何一台無線用戶都不可以連接上路由器。

本頁可用來掃描無線區域網路中的無線基地台的存在，不過只有與路由器相同頻道的無線基地台可以被發現，請按搜尋按鈕尋找所有相連的無線基地台。

無線區域網路 >> 搜尋無線基地台

無線基地台列表

BSSID 頻道 SSID

掃描

查看 統計.

附註在搜尋過程中 (少於5秒)，無線站台將無法和基地台連線。

新增 WDS 設定：

無線基地台的MAC位址 : : : : : 新增

如果您想要找到套用 WDS 設定的無線基地台，請在本頁底部輸入該 AP 的 MAC 位址，然後按加入，稍後該 MAC 位址即會加入 WDS 設定頁面中。

3.10.7 無線用戶端列表

無線用戶端列表提供您目前相連之無線用戶的狀態碼，下圖針對狀態碼提供了詳盡的解說，爲了能有更方便的連線控制，您可以選擇一台 WLAN 用戶站然後選擇**新增到連線控制**，這樣就可以了。

無線區域網路 >> 無線用戶端列表

無線用戶端列表

狀態 MAC 位址

更新頁面

狀態碼:
C: 已連線, 未加密
E: 已連線, WEP.
P: 已連線, WPA
A: 已連線, WPA2
B: 受到連線控制功能的封鎖
N: 連線中
F: 802.1X 或 WPA/PSK 認證失敗

附註: 使用者成功連線至路由器後可能會無預警關閉。在此種情況下，於連線過期前該使用者仍會出現在清單上。

新增至 連線控制：

客戶端的 MAC 位址 : : : : :

新增

更新頁面	按此鈕更新用戶端的 MAC 位址列表。
新增	按此鈕新增選定之 MAC 位址至**連線控制**。

3.10.8 站台流量控制

本頁可讓使用者控制每個無線用戶端的下載上傳速率，請勾選**啟用**方塊以啟動此功能，速率的範圍介於 100 ~ 30,000 kbps 之間。

無線區域網路 >> 站台流量控制

站台流量控制

☑ 啟用

上傳速率	300 00 Kbps
下載速率	300 00 Kbps

附註:
1. 範圍: 100~30,000 Kbps, 增加量: 100 Kbps.
2. 指定速率可應用於每個無線用戶端

確定 取消

3.11 VLAN

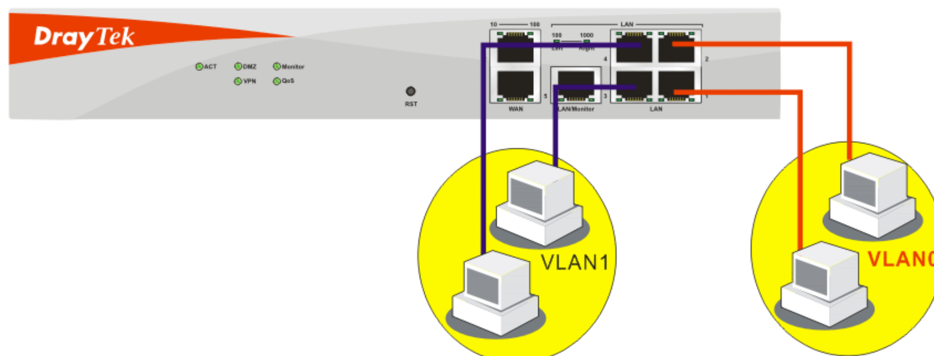
注意: 此功能僅供 **Vigor2950G** 使用，若您是 Vigor2950 的用戶，請參考 3.2.4 一節。

虛擬區域網路的功能提供您一個方便的方式，藉由群組實體通訊埠上的連結主機達到管理的目的。



3.11.1 有線 VLAN

連接上乙太網路連接埠的電腦可以區分成不同的群組且形成虛擬區域網路，在相同群組下的電腦可以透過路由器共享彼此的資訊，且不會受到其他群組的影響。



VLAN >> Wired VALN 允許您透過有線連接的方式，來設定虛擬區域網路設定以達成上述的目的。只要簡單的勾選 VLAN0 該行的 P1 和 P2 方塊，以及 VLAN1 該行的 P3 和 P4 方塊即可。

VLAN >> 有線 VLAN 設定

有線 VLAN 設定

☑ 啟用

	P1	P2	P3	P4
VLAN0	☐	☐	☐	☐
VLAN1	☐	☐	☐	☐
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

確定 清除 取消

啓用	勾選此方塊啓用此功能。
P1 – P4	勾選方塊讓連結至連接埠上的電腦都可群組至指定的 VLAN。注意每個通訊埠都可同時在群組在不同的 VLAN，只要您勾選該相對方塊即可，例如您勾選了 VLAN0-P1 和 VLAN1-P1，您可以讓 P1 同時群組在 VLAN0 和 VLAN1 之下。
VLAN0-3	.路由器允許您設定 4 組虛擬的區域網路。

注意:.如果 WAN2 介面已啓動，P1 方塊將成爲 WAN 介面且無法勾選，請參考下圖。

VLAN >> 有線 VLAN 設定

有線 VLAN 設定

☑ 啟用

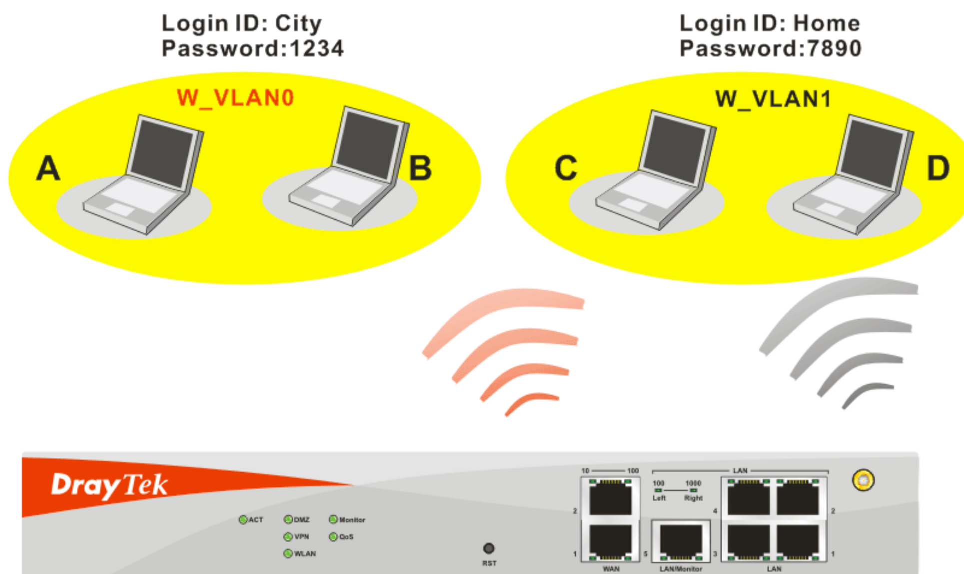
	P1	P2	P3	P4
VLAN0	☐	☐	☐	☐
VLAN1	☐	☐	☐	☐
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

確定 清除 取消

3.11.2 無線 VLAN

經由無線介面連結到路由器且配備無線網路卡的電腦，可以區分成不同的群組並且形成無線的虛擬區域網路，在相同群組下的電腦可以透過路由器共享彼此的資訊，且不會被其他群組窺視。

在相同群組下的電腦可以使用同樣的登入 ID 和密碼，存取網際網路的資訊。例如下圖所示，A 和 B 使用同樣的登入 ID(City)和密碼(1234)，因此他們是群組在相同的無線虛擬區域網路。



VLAN >> Wireless VALN 允許您設定經由無線連線來建立無線虛擬區域網路，以達成上述的目的，只要在 W_VLAN0 的登入 ID 和密碼欄位輸入 **City** 和 **1234**，然後在 W_VLAN1 登入 ID 和密碼碼欄位輸入 **Home** 和 **7890**。在此頁面上，使用者可以設定 14 組無線虛擬區域網路。

VLAN >> 無線 VLAN 設定

無線 VLAN 設定

☑ 啟用　　　　檢視 已連線主機列表

W_VLAN	登入ID	密碼	特性	W_VLAN	登入ID	密碼	特性
0	City	1234	詳情	8			詳情
1	Home	7890	詳情	9			詳情
2			詳情	10			詳情
3			詳情	11			詳情
4			詳情	12			詳情
5			詳情	13			詳情
6			詳情	14			詳情
7			詳情	15			詳情

☐ 停用廣播及多點廣播

附註:
1. 登入 ID: 1~11 字元, 密碼: 1~11 字元
2. 關閉廣播和多點廣播，以增強無線VLAN 安全性。但無線網路的傳輸速率將因此降低。
3. 無線用戶登入URL:
http://www.draytek.vlan/login.htm 或 http://(Vigor路由器IP位址)/login.htm

確定　取消

啓用	勾選此方塊啓用無線虛擬區域網路功能。
登入 **ID**	輸入登入 ID 以應不同的 W_VLAN 群組，ID 字元數字從 1 到 11 個。
密碼	輸入密碼以應不同的 W_VLAN 群組，ID 字元數字從 1 到 11 個。

詳情	勾選此按鈕調整額外的 W_VLAN 設定。

VLAN >> 無線 VLAN 設定

W_VLAN0 特性

啟用時間: 2000 1 1

終止時間: 2007 1 1

以 VLAN 群組連接所有的 WDS 連線

隔離 VLAN 群組中的每個成員

確定 取消

啟用時間 –使用下拉式選項設定無線 VLAN 的啟用時間，無線 VLAN 功能在時間到達時即生效。

終止時間 –使用下拉式選項設定無線 VLAN 的終止時間，無線 VLAN 功能在時間到達時即可失效。

以 **VLAN 群組連接所有的 WDS 連線**–勾選此方塊以啓用連線。

隔離 VLAN 群組中的每個成員–勾選此方塊以隔離所有 VLAN 群組中的成員，且可讓彼此之間的成員無法分享資訊。

停用廣播及多點廣播	勾選此方塊防止廣播及多點廣播至所有的 W_VLAN。

如何(無線用戶端)存取網際網路?

在完成無線 VLAN 的設定之後，連接至此路由器的無線用戶必須完成下列步驟才能存取網際網路。

1. 開啓瀏覽器並在位址欄輸入 http://www.draytek.vlan/login.htm 或 http://(vigor 路由器的 IP 位址)/login.htm。
2. 登入畫面出現如下。

DrayTek Wireless VLAN

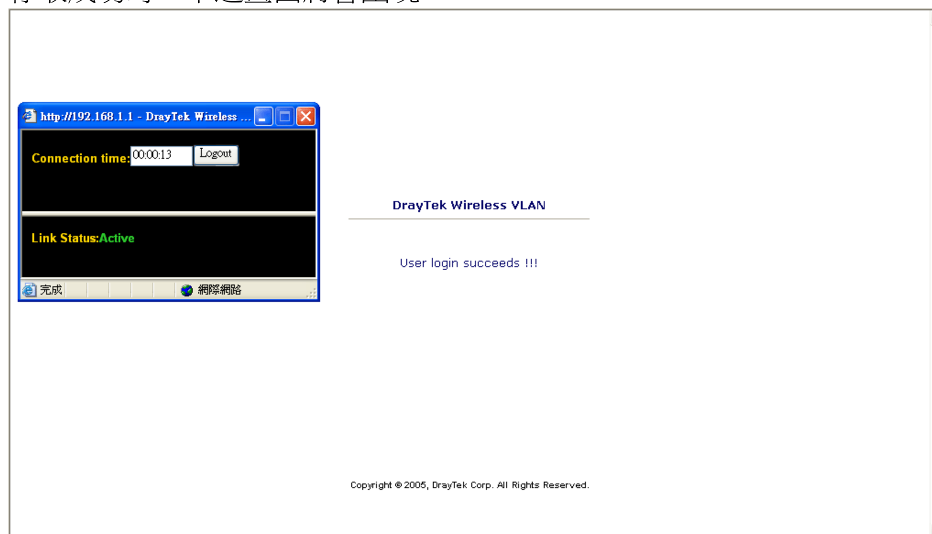
Login ID City

Password ●●●●

OK

3. 輸入無線 VLAN 設定頁面中所載明的登入 ID 和密碼，在本例中，我們選擇第一組設定(City 和 1234)。

4. 存取成功時，下述畫面將會出現。



注意:包含連線時間的浮動視窗將會顯示在螢幕上直到您登出爲止。

5. 您可以前往**自我診斷工具>>無線 VLAN 線上主機列表**檢視連線狀態。

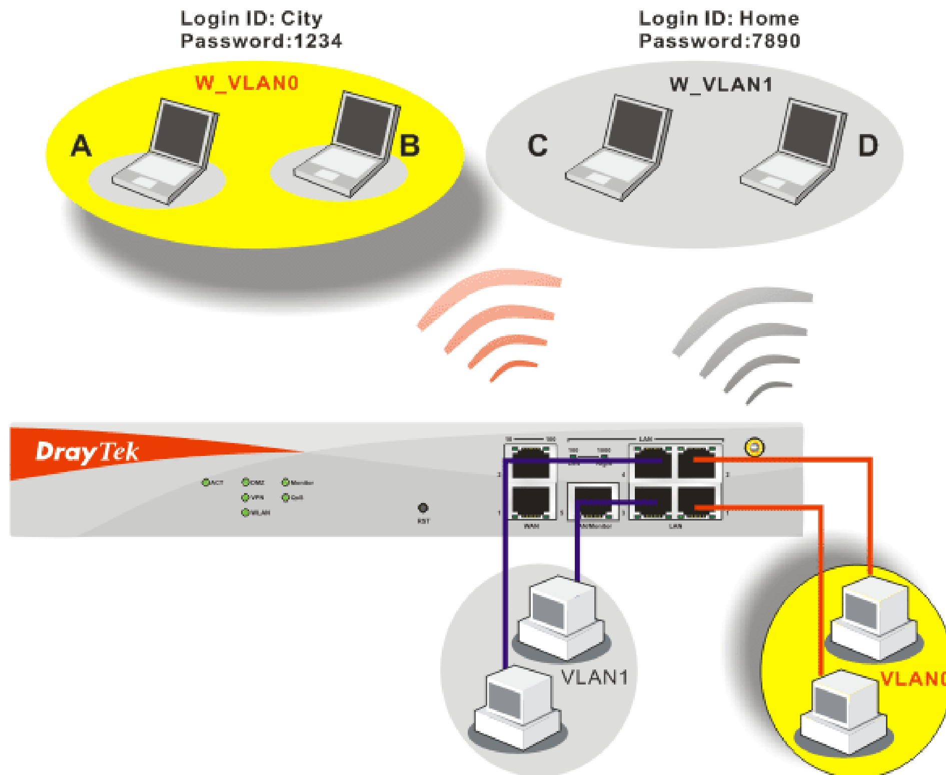
自我診斷工具 >> 無線VLAN線上主機

無線 VLAN 線上主機列表 | **更新頁面** |

IP Address	MAC Address	Login ID
192.168.1.15	00-14-85-26-00-8C	City
192.168.1.16	00-0E-35-A8-A4-E7	Home

3.11.3 VLAN 交叉設定

此功能允許路由器整合 VLAN 和 W_VLAN 以便管理不同的電腦，參考下圖範例，透過此項功能，筆記型電腦 A/B 和 VLAN0 上的電腦可以毫無困難的共享資源。



VLAN >> VALN 交叉設定允許您設定無線 VLAN 和有線 VLAN 間的電腦一個溝通的橋樑，如果要達成圖上的目的，您只要勾選位在 W_VLAN0 行與 VLAN0 之下的方塊即可。

VLAN >> VLAN 交叉設定

VLAN 交叉設定

☐ 啟用

	VLAN0	VLAN1	VLAN2	VLAN3
W_VLAN0	☐	☐	☐	☐
W_VLAN1	☐	☐	☐	☐
W_VLAN2	☐	☐	☐	☐
W_VLAN3	☐	☐	☐	☐
W_VLAN4	☐	☐	☐	☐
W_VLAN5	☐	☐	☐	☐
W_VLAN6	☐	☐	☐	☐
W_VLAN7	☐	☐	☐	☐
W_VLAN8	☐	☐	☐	☐
W_VLAN9	☐	☐	☐	☐
W_VLAN10	☐	☐	☐	☐
W_VLAN11	☐	☐	☐	☐
W_VLAN12	☐	☐	☐	☐
W_VLAN13	☐	☐	☐	☐
W_VLAN14	☐	☐	☐	☐
W_VLAN15	☐	☐	☐	☐
WDS	☐	☐	☐	☐

附註:
1. W_VLAN : 無線 VLAN, 查看 **無線 VLAN 設定** 詳情。
2. 所有的 WDS 連線均歸類於同一個 VLAN 群組。
3. VLAN: 有線 VLAN, 查看 **有線 VLAN 設定** 詳情。
4. 若要使用 VLAN 交叉設定, 有線和無線 VLAN 都必須先啟用。

確定 取消

啟用	勾選此方塊啟用此功能。
VLAN0-3	表示乙太網路介面所連結的虛擬區域網路等群組。
W_VLAN0-15	表示無線介面所溝通的無線 VLAN 群組。

3.11.4 無線流量控制

流量控制可管理資料進出路由器的傳送速度，您也可以管理每個無線 VLAN 的進出速率。至 **VLAN** 功能表中選擇**無線流量控制**，下述設定頁面即可出現。按下**啟用**方塊以啟動 VLAN 功能。

VLAN >> 無線 VLAN 流量控制

無線 VLAN 流量控制

☑啟用　　**範圍**：100~30,000 Kbps, **增加量**：100 Kbps

W_VLAN	上傳速率 (Kbps)	下載速率 (Kbps)	W_VLAN	上傳速率 (Kbps)	下載速率 (Kbps)
0	300 00	300 00	8	300 00	300 00
1	300 00	300 00	9	300 00	300 00
2	300 00	300 00	10	300 00	300 00
3	300 00	300 00	11	300 00	300 00
4	300 00	300 00	12	300 00	300 00
5	300 00	300 00	13	300 00	300 00
6	300 00	300 00	14	300 00	300 00
7	300 00	300 00	15	300 00	300 00

附註：指定速率為VLAN群組的整體系統速率

確定　取消

啓用	勾選此方塊以啓用此功能，流量控制將會限制上傳與下載的傳送量。
上傳速率	表示資料輸出的速率，預設值爲 300，範圍介於 100 kbp 到 20,000kbps，請依照需要調整數值。
下載速率	表示資料輸入的速率，預設值爲 300，範圍介於 100 kbp 到 20,000kbps，請依照需要調整數值。

3.12 系統維護

系統設定方面，有數種項目是使用者需要了解的：系統狀態、系統管理員密碼、備份組態、系統紀錄/郵件警示、時間設定、重啓系統及韌體升級等等。

下圖爲系統維護的主要設定功能。



3.12.1 系統狀態

系統狀態提供基本的網路設定，包含區域網路和 WAN 介面等資訊，同時您也可以獲得目前執行中的韌體版本或是韌體其他的相關資訊。

系統狀態

型號名稱	: Vigor2950 series
韌體版本	: v3.0.0
建立日期/時間	: Mon Sep 11 15:14:40.94 2006

區域網路	
MAC 位址	: 00-50-7F-C0-2F-F4
第一個 IP 位址	: 192.168.1.1
第一個子網路遮罩	: 255.255.255.0
DHCP 伺服器	: 是
DNS	: 194.109.6.66

WAN 1	
連線狀態	: 連線中
MAC 位址	: 00-50-7F-C0-2F-F5
連線	: Static IP
IP 位址	: 172.16.3.229
預設閘道	: 172.16.3.4

WAN 2	
連線狀態	: 斷線
MAC 位址	: 00-50-7F-C0-2F-F6
連線	: ---
IP 位址	: ---
預設閘道	: ---

型號名稱	顯示路由器的型號名稱。
韌體版本	顯示路由器的韌體版本。
建立日期與時間	顯示目前韌體建立的日期與時間。
特徵碼版本	顯示路由器的目前使用的特徵碼版本。
特徵碼建立日期	顯示目前使用的特徵碼建立的日期與時間。
MAC 位址	顯示區域網路介面的 MAC 位址。
第一個 **IP** 位址	顯示區域網路介面的 IP 位址。
第一個子網路遮罩	顯示區域網路介面的子網路遮罩位址。
DHCP 伺服器	顯示區域網路介面的 DHCP 伺服器目前的狀態。
MAC 位址	顯示 WAN 介面的 MAC 位址。
IP 位址	顯示 WAN 介面的 IP 位址。
預設閘道	顯示預設閘道指定的 IP 位址。
DNS	顯示主要 DNS 的 IP 位址。
MAC 位址	顯示無線區域網路的 MAC 位址。

3.12.2 系統管理員密碼

本頁允許您設定新的密碼。

系統維護 >> 系統管理員密碼設定

系統管理員密碼

舊密碼	
新密碼	
確認密碼	

確定

舊密碼	請輸入舊密碼，出廠預設值是空白的。
新密碼	請在本區輸入新密碼。
確認密碼	再次輸入新密碼以確認。

當您按下確定鍵後，登入視窗將會出現，請使用新的密碼以便再次存取網頁設定頁面。

3.12.3 設定備份

設定備份

請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

系統維護 >> 備份設定

備份/還原組態設定

還原

選取一個設定檔。

瀏覽...

按一下"還原"上傳檔案。

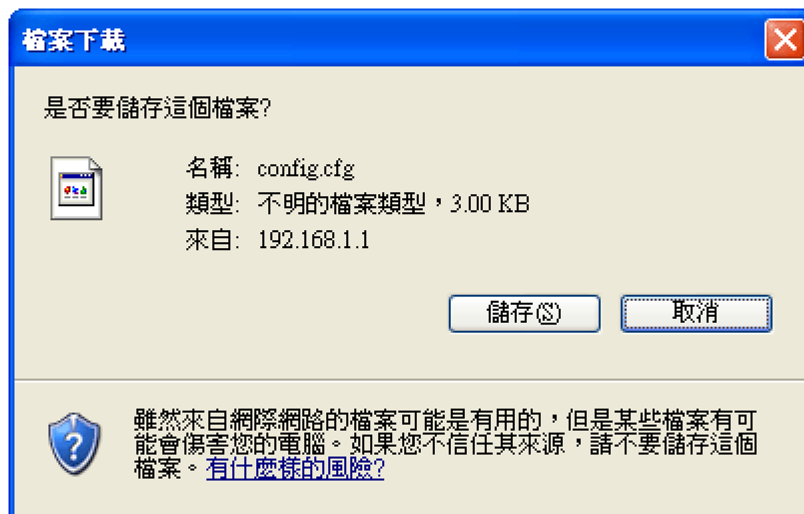
還原

備份

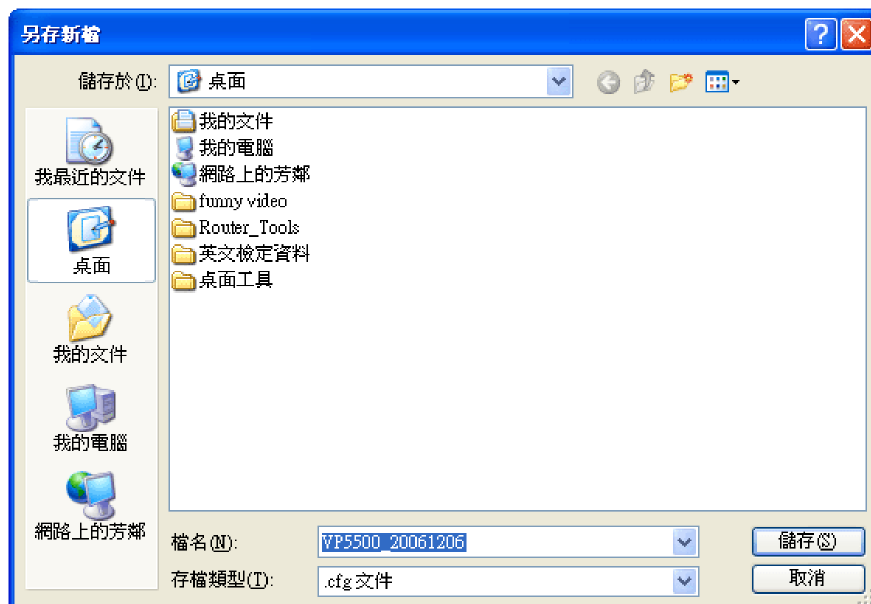
按一下"備份"下載目前的設定檔。

備份 取消

2. 按**備份**按鈕進入下一個對話盒，按**儲存**按鈕開啟另一個視窗以儲存設定。



3. 在**另存新檔**對話盒中，您也可以在此輸入不同的檔名。



4. 按下**儲存**按鈕，設定將會以檔名 **config.cfg** 自動下載至電腦上。

上述範例是以 Windows 平台來完成，對於 **Mac** 或是 **Linux** 平台的用戶，螢幕上將會出現不一樣的視窗，但是備份的功能仍是有效的。

附註:憑證備份須以另一種方式來儲存，備份設定並不包含憑證資訊。

還原設定

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

系統維護 >> 備份設定

備份/還原組態設定

還原

選取一個設定檔。

瀏覽...

按一下"還原"上傳檔案。

還原

備份

按一下"備份"下載目前的設定檔。

備份 取消

2. 按**瀏覽**按鈕選擇正確的設定檔案，以便上傳至路由器。
3. 按**還原**按鈕並等待數秒鐘，下述畫面出現即告訴您還原動作已成功。

3.12.4 SysLog/郵件警示設定

SysLog 在 Unix 系統中是很受歡迎的一種工具，如果要監視路由器的運作狀態，您可以執行 SysLog 程式擷取路由器上所有的活動。此依程式可以在本地電腦或是網際網路上任一遠端電腦上執行，此外 Vigor 路由器提供郵件警示功能，這樣 SysLog 訊息可以郵件方式打包寄給資訊管理人員。

系統維護 >> Syslog / 郵件警示設定

Syslog / 郵件警示設定

Syslog 存取設定

☑ 啟用

伺服器 IP 位址

目標通訊埠 514

啟用 Syslog 訊息:

☐ 防火牆記錄

☐ VPN 記錄

☐ 使用者網路存取紀錄

☐ 通話紀錄

☐ WAN 記錄

☐ 路由器/DSL資訊

郵件警示功能設定

☑ 啟用

SMTP 伺服器

收件人

回信地址

☐ 驗證

使用者名稱

密碼

確定 清除 取消

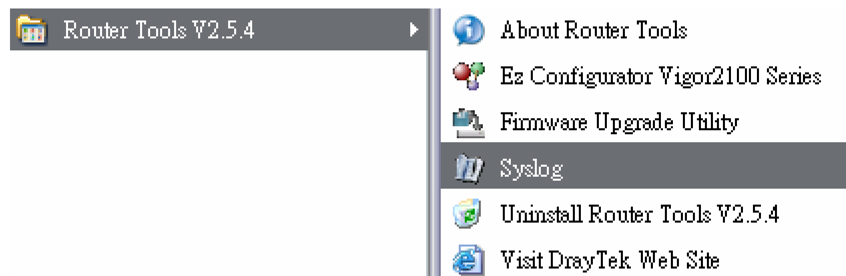
欄位	說明
啓用	勾選**啓用**以啓動系統記錄服務功能。
伺服器 **IP** 位址	指定全部系統紀錄訊息傳送前往目的地之 IP 位址。
目標通訊埠	指定全部系統紀錄訊息傳送前往目的地之通訊埠。
啓用 **Syslog** 訊息	指定 Syslog 顯示的各項紀錄。
SMTP 伺服器	指定 SMTP 伺服器的 IP 位址，直接傳送來自 Vigor 路由器的郵件至收信人的信箱。

收件人	指定收信人信箱的郵件地址，全部的系統紀錄訊息將會自動傳送至此處。收信人可以是想要檢視或是分析系統紀錄訊息的管理人員。
回信地址	指定另一組信箱的郵件地址，接收因收信人信箱錯誤而造成發生失敗的所有回覆訊息 。
驗證	當使用電子郵件應用程式，勾選此方塊可啓動驗證的功能。
使用者名稱	輸入驗證所需的使用者名稱。
密碼	輸入驗證所需的密碼。

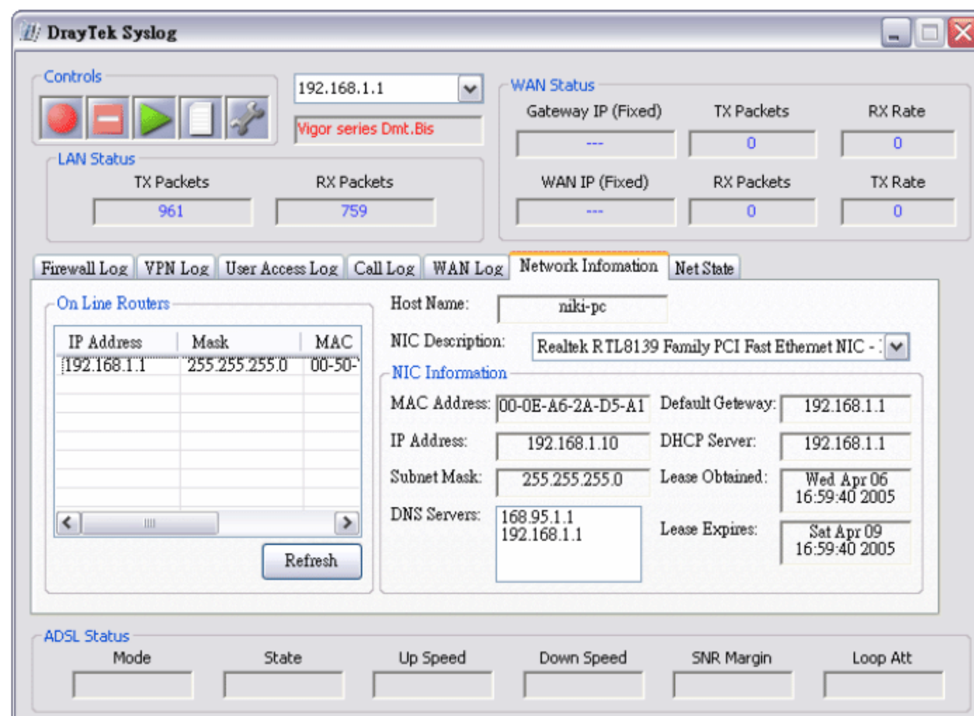
按**確定**儲存所有的設定。

如欲檢視系統紀錄，請依照下述步驟進行：

1. 請在伺服器 IP 地址中設定監視電腦的 IP 地址。
2. 安裝光碟片中 **Utility** 下的路由器工具，安裝完畢後，請自程式集選取 **Router Tools>>Syslog**。



3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在網路資訊(**Network Information)**中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。



3.12.5 時間和日期

允許您指定自何處取得路由器時間。

系統維護 >> 時間與日期

時間資訊

目前系統時間	2000 Jan 1 Sat 0 : 24 : 43	取得時間

時間設定

○ 使用本台PC的時間

◉ 使用網際網路時間伺服器

時間協定	NTP (RFC-1305)
伺服器 IP 位址	pool.ntp.org
時區	(GMT) 格林威治標準時間:都柏林
啟用日光節約時間	☐
自動更新間隔	30分鐘

確定　取消

目前系統時間	按**取得時間**按鈕取得目前時間。
使用本台 **PC** 的時間	選擇此項以便採用遠端管理者電腦上的瀏覽器時間，作。
使用網際網路的時間伺服器	選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。
時間協定	選擇適合本地的時間協定。
伺服器 **IP** 位址	輸入時間伺服器的 IP 地址。
時區	選擇路由器所在的時區。
啓用日光節約時間	勾選此項目可啓用日光節約時間。這個功能主要是提供給歐洲地區國家使用，並非適用於台灣地區。
自動更新間隔	選定時間間隔以供 NTP 伺服器更新之用。

全部設定完成之後請按**確定**儲存目前的設定。

3.12.6 管理

本頁讓您管理存取控制、存取清單、通訊埠設定以及 SNMP 設定。例如管理存取控制時，埠號用來傳送/接收 SIP 訊息以便建立連線。

系統維護 >> 管理

管理設定

管理存取控制

啟用遠端韌體更新（FTP）

允許從網際網路管理

斷絕來自外部網際網路的PING

存取清單

清單 IP 子網路遮罩

1

2

3

管理通訊埠設定

預設通訊埠

(Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)

使用者定義通訊埠

Telnet通訊埠 23

HTTP 通訊埠 80

HTTP 通訊埠 443

FTP 通訊埠 21

SNMP 設定

啟用 SNMP 代理程式

取得社群(Get Community) public

設定社群(Set Community) private

管理者主機 IP

封鎖社群(Trap Community) public

通知主機 IP

封鎖逾時 10 秒

確定

啓用遠端韌體更新(FTP)	勾選此方塊允許透過 FTP 執行遠端韌體更新。
允許從網路管理	勾選此方塊允許系統管理者自網際網路登入。此項預設值是不允許的。
斷絕來自網際網路的 PING	勾選此方塊以退回所有來自網際網路的 PING 封包，考量到安全性問題，這項功能的預設值是啓動的。
存取清單	您可以指定系統管理者只能從指定的主機或是清單定義的網路上登入，您一次最多可定義三個 IP/子網路遮罩於此區域中。 **清單 IP** – 指定一個允許登入至路由器的 IP 地址。 **子網路遮罩** -代表允許登入至路由器的子網路遮罩。
預設通訊埠	勾選此項以使用標準埠號作爲 Telnet 和 HTTP 伺服器之用。
使用者定義通訊埠	勾選此項以指定使用者定義的埠號作爲 Telnet、HTTP、HTTPS、FTP 伺服器之用。
啓用 SNMP 代理程式	勾選此項以啓動此功能。

取得社群 **(Get Community)**	請輸入適當的文字以設定取得社群名稱，預設名稱為 **public**。
設定社群 **(Set Community)**	請輸入適當的名稱以設定社群，預設名稱為 **private**。
管理者主機 **IP**	設定一台主機做為管理者以便執行 SNMP 功能，請輸入 IP 位址指定特定主機。
封鎖社群**(Trap Community)**	輸入適當名稱設定封鎖社群，預設名稱為 **public**。
通知主機 **IP**	設定主機的 IP 地址接收封鎖社群的資料。
封鎖逾時	預設值為 10 秒。

3.12.7 重啓路由器

網路設定可以用來重新啓動路由器，請自**系統維護**中按**重啓路由器**開啓如下頁面。

系統維護 >> 重啟路由器

重啟路由器

您想重新啟動路由器嗎？

- ◉ 使用目前組態
- ○ 使用原廠預設組態

確定

如果您想要使用目前的設定來重新啓動路由器，請勾選**使用目前組態**，然後按**確定**；如果要重設路由器設定回復成為預設值，請勾選**使用原廠預設組態**，然後按**確定**，路由器將會花 5 秒重新啓動系統。

> **注意:**.當系統在您完成網頁設定並跳出**重啓路由器**網頁後，請務必按下**確定**以重新啓動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

3.12.8 韌體升級

在您更新路由器韌體之前，您必須先行安裝路由器工具。**韌體更新工作**即包含在此工具內，以下的網頁透過範例說明引導您更新韌體，注意此範例是在 Windows 操作系統下完成。

自居易網站或是 FTP 站下載最新的韌體版本，居易網站為 www.draytek.com，FTP 站則是 ftp.draytek.com。

請自**系統維護**選擇**韌體升級**以便啓動韌體更新工具。

系統維護 >> 韌體升級

網頁韌體升級

選擇韌體檔案

[瀏覽...]

按升級以上傳檔案。 [升級]

從LAN端執行 TFTP 韌体升級

目前韌體版本: v3.0.0

韌體升級程序:

- 1. 按 "確定" 開啟 TFTP 伺服器。
- 2. 開啟韌體升級公用程式或其它協力廠商 TFTP 用戶端軟體。
- 3. 檢查韌體檔名是否正確。
- 4. 按下韌體更新工具的 "Upgrade" 按鈕啟動更新作業。
- 5. 升級完成後，TFTP 伺服器將自動停止執行。

您確定要升級韌體嗎？ [確定]

按**確定**，下述畫面將會出現，請先使用韌體更新工具完成更新。

系統維護 >> 韌體升級

TFTP 伺服器運作中。請執行韌體升級公用程式以升級路由器的韌體。當韌體升級完成後，此伺服器將自行關閉。

有關韌體更新的詳細資訊，請參考第五章。

3.13 自我診斷工具

自我診斷工具提供一個非常有效的方式，讓使用者能夠檢視或是診斷路由器的現況。以下為自我診斷的選單項目：



3.13.1 撥號觸發器

按自我診斷工具的**撥號觸發器**開啟網頁，網際網路連線(如 PPPoE 或 PPPoA)可由來源 IP 位址封包來觸發。

自我診斷工具 >> 撥號觸發器

已觸發的撥出封包標頭 | 更新頁面 |

HEX 格式:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

已解碼格式:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

已解碼格式	顯示來源 IP 位址、目標 IP 位址、通訊協定和封包的長度。
更新頁面	按此鈕重新載入本頁。

3.13.2 路由表

按自我診斷工具的路由表檢視路由器的路由表格，此表格可提供目前的 IP 路由資訊。

自我診斷工具 >> 檢視路由表

目前執行中的路由表 | 更新頁面 |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*          0.0.0.0/         0.0.0.0 via 172.16.3.4,    WAN1
C~       192.168.1.0/   255.255.255.0 is directly connected,    LAN
C         172.16.0.0/     255.255.0.0 is directly connected,   WAN1
```

更新頁面　　按此鈕重新載入本頁。

3.13.3 ARP 快取表

按自我診斷工具的 **ARP** 快取表檢視路由器中 ARP(Address Resolution Protocol)快取的內容，此表格顯示乙太網路硬體位址(MAC 位址)和 IP 位址間的對應狀況。

自我診斷工具 >> 檢視 ARP 快取表

乙太網路 ARP 快取表 | 清除 | 更新頁面 |

```
IP Address          MAC Address
192.168.1.10        00-0E-A6-2A-D5-A1
172.16.2.141        00-15-F2-BC-21-91
172.16.2.111        00-0E-A6-39-D1-C0
172.16.2.156        00-E0-18-BE-A6-EF
172.16.2.213        00-50-7F-30-1E-E9
172.16.2.109        00-0C-6E-05-16-F9
172.16.3.200        00-10-B5-3A-32-3C
172.16.2.18         00-50-FC-2F-3D-17
172.16.2.133        00-0C-6E-5E-C8-0C
172.16.3.204        00-50-7F-25-FA-4D
172.16.2.181        00-0E-A6-2A-D5-EF
172.16.2.236        00-50-7F-12-55-77
172.16.3.163        00-50-7F-1A-58-89
172.16.3.198        00-50-7F-1A-57-AE
172.16.3.156        00-50-7F-1A-56-0E
```

更新頁面　　按此鈕重新載入本頁。

清除　　按此連結清除整個表格。

3.13.4 DHCP 表

此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。

按下自我診斷工具，選擇 **DHCP 表**開啓相關網頁。

自我診斷工具 >> 檢視 DHCP 指派的 IP 位址

DHCP IP 指派表 | 更新頁面 |

```
DHCP server: Running
Index    IP Address        MAC Address                 Leased Time       HOST ID
```

Index 顯示連線項目編號。

IP Address 顯示路由器指派給特定電腦的 IP 位址。

MAC Address 顯示 DHCP 指派給特定電腦的 MAC 位址。

Leased Time 顯示指定電腦的租約時間。

HOST ID 顯示指定電腦的主機 ID 名稱。

更新頁面 按此鈕重新載入本頁。

3.13.5 NAT 連線數狀態表

按下自我診斷工具，選擇 **NAT 連線數狀態表**開啓相關網頁。

自我診斷工具 >> NAT 連線數狀態表

NAT 連線數狀態表 | 更新頁面 |

```
------------------------------------------------------------------------------------
    Private IP :Port #Pseudo Port         Peer IP :Port  Interface
------------------------------------------------------------------------------------
  192.168.1.10  1374        50960   207.46.106.13     80     WAN1
  192.168.1.10  1381        50967   207.46.26.254   7001     WAN1
  192.168.1.10  1381        50967   207.46.26.254      9     WAN1
  192.168.1.10  1381        50967   207.46.26.253   7001     WAN1
```

Private IP:Port	本機電腦的 IP 位址和埠號。
#Pseudo Port	路由器爲了執行 NAT 所使用的暫時通訊埠。
Peer IP:Port	遠端主機的目標 IP 位址與埠號。
Interface	代表 WAN 連線介面
更新頁面	按此鈕重新載入本頁。

3.13.6 無線 VLAN 線上主機列表

按下**診斷工具**，選擇**無線 VLAN 線上主機列表**開啓相關網頁。本頁顯示所有無線 VLAN 主機的 IP 位址、MAC 位址和登入 ID 資訊。

自我診斷工具 >> 無線VLAN線上主機

無線 VLAN 線上主機列表 | 更新頁面 |

IP Address	MAC Address	Login ID
192.168.1.15	00-14-85-26-00-8C	City
192.168.1.16	00-0E-35-A8-A4-E7	Home

IP Address	顯示無線主機的 IP 位址。
MAC Address	顯示無線主機的 MAC 位址。
Login ID	顯示無線主機所屬的登入 ID。

3.13.7 資料流量監控

本頁顯示所監視的 IP 位址執行的過程，並在數秒的間隔後重新更新頁面，此處所列出的 IP 位址是在頻寬管理中設定完成的，在啟動資料流量監控之前，您必須啟動 IP 頻寬限制以及 IP 連線數限制。若沒有這麼做的話，系統會出現知會畫面提醒您先啟動相關設定。

頻寬管理 >> NAT 連線數限制

NAT 連線數限制

啟用　停用

預設最大連線數: 100

限制清單

索引　起始 IP　結束

按下**自我診斷工具**，選擇**資料流量監控**開啟相關網頁。

自我診斷工具 >> 資料流量監控

啟用資料流量監控

排列依據: IP　更新秒數: 5　頁: 1　| 更新頁面 |

索引編號	IP 位址	傳送速率(Kbps)	接收速率(Kbps)	NAT 連線數	動作

附註: 1. 按"封鎖"防止指定 PC 存取網際網路 5 分鐘。
2. 路由器封鎖的 IP 以紅色顯示，NAT 連線欄位顯示該IP解除封鎖之剩餘時間(秒數)。

啟用資料流量監控　　勾選此方塊以啟動此功能。

排列依據　　請使用下拉式選項選擇排列資料的順序。

排列依據: IP

IP
傳送
接收
NAT 連線數

更新秒數	使用下拉式選項選擇系統自動更新資料的間隔時間。 更新秒數: 5 5 10 15 30
更新頁面	按此連結更新本頁。
索引	顯示資料流量的項目筆數。
IP 位址	顯示被監視裝置的 IP 位址。
傳送速率 (kbps)	顯示被監視裝置的傳送速率。
接收速率 (kbps)	顯示被監視裝置的接收速率。
NAT 連線數	顯示您在連線數限制網頁中所設定的連線數。
動作	封鎖 – 可以避免指定電腦在 5 分鐘內存取網際網路。 頁: 1 | 更新頁面 | 率(Kbps) NAT 連線數 動作 13 1 封鎖 解除 – 指定 IP 位址的裝置將在五分鐘內封鎖起來，剩餘時間將顯示在 NAT 連線數欄位中。 頁: 1 | 更新頁面 |) NAT 連線數 動作 blocked / 299 解除

3.13.8 流量圖表

按下**自我診斷工具**，選擇**流量圖表**開啓相關網頁。可以選擇 **WAN1 頻寬/WAN2 頻寬**或是**連線數**來檢視流量圖表。您可隨時按**更新頁面**重新顯示圖表內容。

自我診斷工具 >> 流量圖表



水平軸代表時間；而垂直軸代表的意義就很不同了。對 **WAN1 頻寬/WAN2 頻寬**而言，垂直軸代表的是過去所傳送與接收封包的數量。但對**連線數**來說，垂直軸代表的是過去一段時間之內的 NAT 連線數。

3.13.9 Ping 自我診斷

按下**自我診斷工具**，選擇 **Ping 自我診斷**開啓相關網頁。

自我診斷工具 >> Ping 診斷

Ping 診斷

附註: 如果您想要 Ping 區域網路上的電腦，或是不想指定經由哪個 WAN 介面來執行 ping 動作，請選擇 "不指定"。

經由介面: 不指定

Ping 至: 主機 / IP　　IP 位址:

執行

執行結果　　清除

經由介面　　使用下拉式清單選擇您想要經由該介面來 ping 裝置的 WAN 介面，或是選擇**不指定**由路由器自動挑選適合的介

面。

經由介面: 不指定
不指定
WAN1
WAN2

Ping 至	使用下拉式清單選擇您想要 Ping 的目標。 Ping 至: 主機 / IP 主機 / IP 閘道 1 閘道 2 DNS
IP 位址	輸入您想要 Ping 的主機/IP 上的 IP 位址。
執行	按此鈕啟動 Ping 作業，結果將會顯示在螢幕上。
清除	按此連結清除視窗上的結果。

3.13.10 追蹤路由

按下**自我診斷工具**，選擇**追蹤路由**開啟相關網頁。本頁允許您追蹤路由器至主機之間的路由情況，只要簡單的輸入主機的 IP 位址並按下執行按鈕，整個路由狀況都將顯示在螢幕上。

自我診斷工具 >> 追蹤路由

追蹤經由介面

追蹤經由介面: 不指定

主機 / IP 位址: [ ] 執行

執行結果 | 清除 |

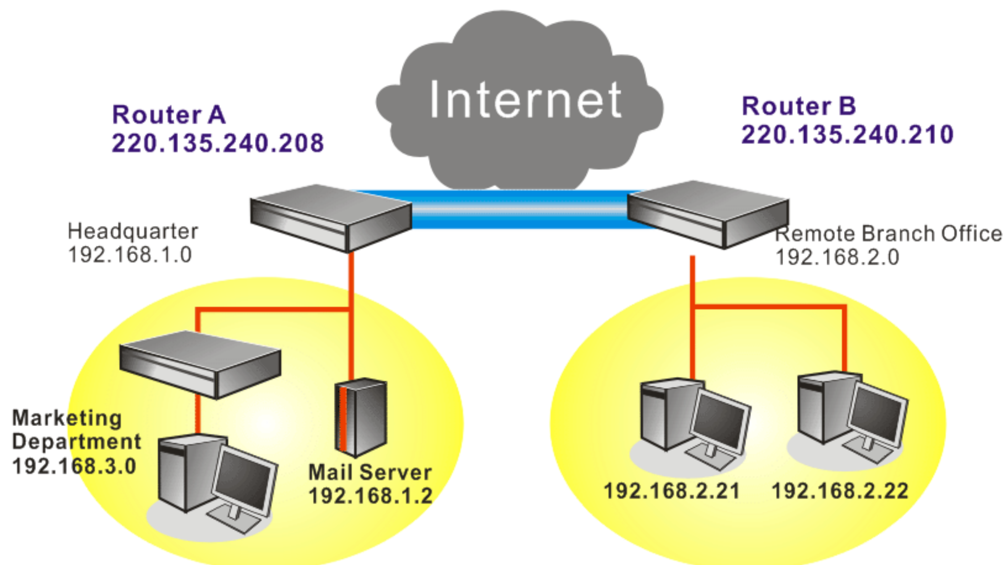
```
Trace through WAN1.
traceroute to 192.168.1.1, 30 hops max
  1 Request timed out.     *
  2 Request timed out.     *
Trace complete.
```

追蹤經由介面	使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使用**不指定**讓路由器自動決定選擇哪一種介面。 追蹤經由介面: 不指定 不指定 WAN1 WAN2
主機/**IP** 位址	指明主機的 IP 位址。
執行	按此鈕開始路由追蹤動作。
清除	按此連結刪除視窗上的結果。

4 應用與範例

4.1 建立遠端辦公室與總公司之間的 LAN-to-LAN 連線

最常見的範例是例如遠端分公司與總公司之間的安全連線，依照下圖所顯示的網路結構，您可以遵循提供的步驟來建立 LAN-to-LAN 設定檔案，這二個區域網路不可具有相同的網路位址。



在總部辦公室內路由器 A 的設定:

1. 開啟 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啟用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 為主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

VPN 與遠端存取 >> PPP 基本設定

PPP 基本設定

PPP/MP 協定		指派 IP 給撥入使用者	
撥入PPP驗證	PAP 或 CHAP	起始 IP 位址	192.168.1.200
撥入 PPP 加密（MPPE）	選擇 MPPE		
雙方共同驗證（PAP）	○ 是 ⊙ 否		
使用者名稱			
密碼			

確定

針對使用 IPSec 為主的服務，像是 IPSec 或是以 IPSec 原則為主的 L2TP，您必須在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

VPN 與遠端存取 >> IPSec 基本設定

VPN IKE / IPSec 基本設定

遠端撥入使用者及動態 IP 客戶的撥入設定（LAN to LAN）。

IKE 認證方式

預先共用金鑰 ••••

確認預先共用金鑰 ••••

IPSec 安全防護方式

☑ 中級（AH）

對資料進行認證，但不會進行加密。

高級（ESP） ☑ DES ☑ 3DES ☑ AES

對資料進行認證及加密。

確定 取消

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。
4. 將一般設定如下調整，您應該啓動 VPN 連線，因爲任何一方都可啓動 VPN 連線。

VPN 與遠端存取 >> LAN to LAN

設定檔索引：1

1. 一般設定

設定檔名稱 Branch1

☐ 啟用此設定檔

VPN 連線經由介面： WAN1 優先

撥號方向 ⦿ 雙向 ○ 撥出 ○ 撥入

☐ 永遠連線

閒置逾時 300 秒(s)

☐ 啟用 PING 以維持連線

指定 IP 位址

5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

2. 撥出設定

我撥出的伺服器類型

○ ISDN

○ PPTP

⦿ IPSec

○ 具有 IPSec 原則的 L2TP 無

ISDN 撥接號碼或

對方 VPN 所需之伺服器 IP 或域名.

(例如 5551234, draytek.com 或 123.45.67.89)

220.135.240.210

連接類型 64k bps

使用者名稱 ???

密碼

PPP 驗證 PAP/CHAP

VJ 壓縮 ⦿ 開啟 ○ 關閉

IKE 驗證方式

⦿ 預先共用金鑰

IKE 預先共用金鑰 ••••

○ 數位簽章(X.509)

無

IPSec 安全防護方式

⦿ 中級(AH)

○ 高級(ESP) DES 無驗證

進階

索引號碼(1-15) 於 排程 設定:

回撥功能 (CBCP)

☐ 所需回撥的遠端

☐ 提供 ISDN 號碼予遠端

如果選擇是 PPP 爲主的服務項目，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

2. 撥出設定

我撥出的伺服器類型

- ISDN
- PPTP
- IPSec
- 具有 IPSec 原則的 L2TP 無

ISDN 撥接號碼或
對方 VPN 所需之伺服器 IP 或域名.
(例如 5551234, draytek.com 或 123.45.67.89)
220.135.240.210

連接類型 64k bps
使用者名稱 ???
密碼
PPP 驗證 PAP/CHAP
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰 ••••
數位簽章(X.509)
無

IPSec 安全防護方式
中級(AH)
高級(ESP) DES 無驗證
進階

索引號碼(1-15) 於 排程 設定:

回撥功能 (CBCP)
所需回撥的遠端
提供 ISDN 號碼予遠端

6. 將**撥入設定**按下圖所示調整以便路由器 B 建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、認證方式和 IPSec 安全防護方式，否則系統將自動爲您採用上述 **IPSec 一般設定**頁面所定義的設定。

3. 撥入設定

允許的撥入模式

- ISDN
- PPTP
- IPSec
- 具有 IPSec 原則的 L2TP 無

Specify ISDN CLID 或遠端 VPN 閘道
對方 ISDN 號碼或對方 VPN 伺服器 IP
220.135.240.210
或對方 ID

使用者名稱 ???
密碼
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰
數位簽章(X.509)
無

IPSec 安全防護方式
中級 (AH)
高級 (ESP)
DES 3DES AES

回撥功能 (CBCP)
啟用回撥功能
使用下列號碼回撥
回撥號碼
剩餘回撥時間 0 分(s)

如果選擇的是 PPP 爲主的服務項目，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

3. 撥入設定

允許的撥入模式
ISDN
PPTP
IPSec
具有 IPSec 原則的 L2TP 無

Specify ISDN CLID 或遠端 VPN 閘道
對方 ISDN 號碼或對方 VPN 伺服器 IP
220.135.240.210
或對方 ID

使用者名稱 draytek
密碼 •••••••
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰
數位簽章(X.509)
無

IPSec 安全防護方式
中級 (AH)
高級 (ESP)
DES 3DES AES

回撥功能 (CBCP)
啟用回撥功能
使用下列號碼回撥
回撥號碼
剩餘回撥時間 0 分(s)

7. 最後在 **TCP/IP 網路設定**欄位中設定遠端網路 IP/子網路，如此一來，路由器 A 可以透過 VPN 連線直接將封包導引至路由器 B 之遠端網路上。

4. TCP/IP網路設定

我的 WAN IP	0.0.0.0
遠端閘道IP	0.0.0.0
遠端網路 IP	192.168.2.0
遠端網路遮罩	255.255.255.0
	更多

RIP 方向 停用
第一子網段到遠端網路要做 路由
指定此 VPN 通道為預設路由

確定 清除 取消

在遠端辦公室內路由器 **B** 的設定**:**

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下確定。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 一般設定** 調整設定值。

VPN 與遠端存取 >> PPP 基本設定

PPP 基本設定

PPP/MP 協定
撥入PPP驗證 PAP 或 CHAP
撥入 PPP 加密 (MPPE) 選擇 MPPE
雙方共同驗證 (PAP) 是 否
使用者名稱
密碼

指派 IP 給撥入使用者
起始 IP 位址 192.168.2.200

確定

針對使用 IPSec 爲主的服務，像是 IPSec 或是以 IPSec 政策爲主的 L2TP，您必須

在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

VPN 與遠端存取 >> IPSec 基本設定

VPN IKE / IPSec 基本設定

遠端撥入使用者及動態 IP 客戶的撥入設定（LAN to LAN）。

IKE 認證方式

預先共用金鑰 ••••

確認預先共用金鑰 ••••

IPSec 安全防護方式

☑ 中級（AH）

對資料進行認證，但不會進行加密。

高級（ESP） ☑ DES ☑ 3DES ☑ AES

對資料進行認證及加密。

確定 取消

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。
4. 將一般設定如下調整，您應該啓動 VPN 連線，因爲任何一方都可啓動 VPN 連線。

VPN 與遠端存取 >> LAN to LAN

設定檔索引 : 1

1. 一般設定

設定檔名稱	Branch1	撥號方向	⊙ 雙向 ○ 撥出 ○ 撥入
☐ 啟用此設定檔		☐ 永遠連線	
		閒置逾時	300 秒(s)
VPN 連線經由介面:	WAN1 優先	☐ 啟用 PING 以維持連線	
		指定 IP 位址	

5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。

如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

2. 撥出設定

我撥出的伺服器類型

- ISDN
- PPTP
- IPSec
- 具有 IPSec 原則的 L2TP 無

ISDN 撥接號碼或
對方 VPN 所需之伺服器 IP 或域名.
(例如 5551234, draytek.com 或 123.45.67.89)
220.135.240.208

連接類型 64k bps
使用者名稱 ???
密碼
PPP 驗證 PAP/CHAP
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰 •••••
數位簽章(X.509)
無

IPSec 安全防護方式
中級(AH)
高級(ESP) DES 無驗證
進階

索引號碼(1-15) 於 排程 設定:

回撥功能 (CBCP)
所需回撥的遠端
提供 ISDN 號碼予遠端

如果選擇的是 PPP 為主的服務項目，您可以為此撥號連線進一步指定對方 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

2. 撥出設定

我撥出的伺服器類型

- ISDN
- PPTP
- IPSec
- 具有 IPSec 原則的 L2TP 無

ISDN 撥接號碼或
對方 VPN 所需之伺服器 IP 或域名.
(例如 5551234, draytek.com 或 123.45.67.89)
220.135.240.208

連接類型 64k bps
使用者名稱 draytek
密碼 •••••••
PPP 驗證 PAP/CHAP
VJ 壓縮 開啟 關閉

IKE 驗證方式
預先共用金鑰
IKE 預先共用金鑰 •••••
數位簽章(X.509)
無

IPSec 安全防護方式
中級(AH)
高級(ESP) DES 無驗證
進階

索引號碼(1-15) 於 排程 設定:

回撥功能 (CBCP)
所需回撥的遠端
提供 ISDN 號碼予遠端

6. 將**撥入設定**按下圖所示調整以便路由器 A 建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以為此撥號連線進一步指定遠端相對的 IP 位址、認證方式和 IPSec 安全防護方式，否則系統將自動為您採用上述 **IPSec 基本設定**頁面所定義的設定。

3. 撥入設定

允許的撥入模式

ISDN

PPTP

IPSec

具有 IPSec 原則的 L2TP 無

Specify ISDN CLID 或遠端 VPN 閘道

對方 ISDN 號碼或對方 VPN 伺服器 IP

220.135.240.208

或對方 ID

使用者名稱 ???

密碼

VJ 壓縮 開啟 關閉

IKE 驗證方式

預先共用金鑰

IKE 預先共用金鑰

數位簽章(X.509)

無

IPSec 安全防護方式

中級 (AH)

高級 (ESP)

DES 3DES AES

回撥功能 (CBCP)

啟用回撥功能

使用下列號碼回撥

回撥號碼

剩餘回撥時間 0 分(s)

如果選擇的服務項目是 ***PPTP*** 為主的服務，您可以為此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

3. 撥入設定

允許的撥入模式

ISDN

PPTP

IPSec

具有 IPSec 原則的 L2TP 無

Specify ISDN CLID 或遠端 VPN 閘道

對方 ISDN 號碼或對方 VPN 伺服器 IP

220.135.240.208

或對方 ID

使用者名稱 draytek

密碼 •••••

VJ 壓縮 開啟 關閉

IKE 驗證方式

預先共用金鑰

IKE 預先共用金鑰

數位簽章(X.509)

無

IPSec 安全防護方式

中級 (AH)

高級 (ESP)

DES 3DES AES

回撥功能 (CBCP)

啟用回撥功能

使用下列號碼回撥

回撥號碼

剩餘回撥時間 0 分(s)

7. 最後在 **TCP/IP Network Settings** 設定遠端網路 IP/子網路，如此一來，路由器 B 可以透過 VPN 連線直接將封包導引至路由器 A 之遠端網路上。

4. TCP/IP網路設定

我的 WAN IP 0.0.0.0

遠端閘道 IP 0.0.0.0

遠端網路 IP 192.168.1.0

遠端網路遮罩 255.255.255.0

更多

RIP 方向 停用

第一子網段到遠端網路要做

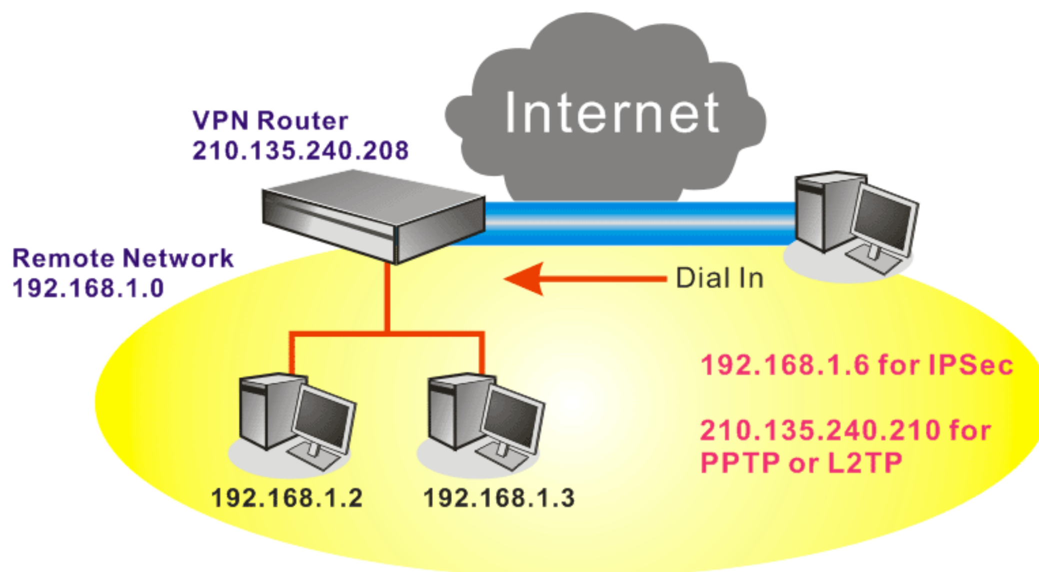
路由

指定此 VPN 通道為預設路由

確定 清除 取消

4.2 建立工作者和總部之間的 VPN 遠端撥號連線

另一個常用的範例是：作爲一個工作者，您可能想要安全地連接到企業網路，依照下面所顯示的網路結構，您可以遵照相關的步驟來建立遠端用戶設定檔，並且在遠端主機上安裝 Smart VPN Client。



在辦公室內VPN路由器的設定:

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

VPN 與遠端存取 >> PPP 基本設定

PPP 基本設定

PPP/MP 協定		指派 IP 給撥入使用者	
撥入PPP驗證	PAP 或 CHAP	起始 IP 位址	192.168.1.200
撥入 PPP 加密 (MPPE)	選擇 MPPE		
雙方共同驗證 (PAP)	○ 是 ⊙ 否		
使用者名稱			
密碼			

確定

如果選擇的服務項目是 ***IPSec***，如 IPsec 或是 IPSec 原則之 L2TP，您必須設定 **IKE/IPSec 基本設定**像是雙方都應知曉的預設共用金鑰。

VPN 與遠端存取 >> IPSec 基本設定

VPN IKE / IPSec 基本設定

遠端撥入使用者及動態 IP 客戶的撥入設定（LAN to LAN）。

IKE 認證方式

預先共用金鑰 ••••

確認預先共用金鑰 ••••

IPSec 安全防護方式

☑ 中級（AH）

對資料進行認證，但不會進行加密。

高級（ESP） ☑ DES ☑ 3DES ☑ AES

對資料進行認證及加密。

確定 取消

3. 至**遠端撥入使用者**，按任一索引編號以編輯設定檔。
4. 將**撥入設定**按下圖所示調整，以便遠端使用者建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以為此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式，否則系統將自動為您採用上述 **IPSec 基本設定**頁面所定義的設定。

VPN 與遠端存取 >> 遠端撥入使用者

索引編號 1

使用者帳號與認證

☑ 開啟這個帳號

閒置逾時 300 秒

使用者名稱 ???

密碼

允許的撥入模式

☐ ISDN

☐ PPTP

☑ IPSec通道

☐ 具有 IPSec 原則的 L2TP 無

☑ 指定遠端節點

遠端用戶或對方 ISDN 號碼

210.135.240.210

或對方 ID

IKE 認證方式

☑ 預先共用金鑰

IKE 預先共用金鑰

☐ 數位簽章 (X.509)

無

IPSec 安全防護方式

☑ 中級 (AH)

高級 (ESP)

☑ DES ☑ 3DES ☑ AES

本機 ID (視需要填入)

回撥功能

☐ 啟動回撥功能

☐ 指定回撥號碼

回撥號碼

☑ 啟動剩餘回撥時間控制

剩餘回撥時間 30 分

確定 清除 取消

如果選擇的是 PPP 爲主的服務項目，您應該爲此撥號連線進一步指定遠端相對的 IP 位址、使用者名稱、密碼以及 VJ 壓縮。

VPN 與遠端存取 >> 遠端撥入使用者

索引編號 1

使用者帳號與認證
☑ 開啟這個帳號
閒置逾時 300 秒

使用者名稱 draytek
密碼 ••••

允許的撥入模式
☐ ISDN
☑ PPTP
☐ IPSec通道
☐ 具有 IPSec 原則的 L2TP 無
☑ 指定遠端節點
遠端用戶或對方 ISDN 號碼
210.135.240.210
或對方 ID

IKE 認證方式
☑ 預先共用金鑰
IKE 預先共用金鑰
☐ 數位簽章 (X.509)
無

IPSec 安全防護方式
☑ 中級 (AH)
高級 (ESP)
☑ DES ☑ 3DES ☑ AES
本機 ID (視需要填入)

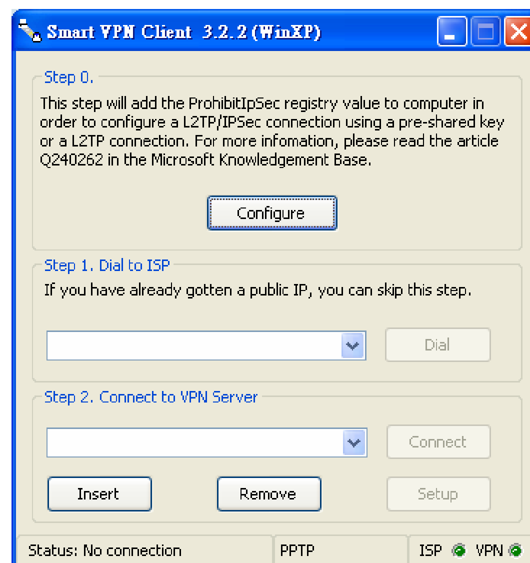
回撥功能
☐ 啟動回撥功能
☐ 指定回撥號碼
回撥號碼
☑ 啟動剩餘回撥時間控制
剩餘回撥時間 30 分

確定 清除 取消

遠端主機上的設定:

1. 對 Win98/ME 系統而言，您可以使用 Dial-up Networking 建立 PPTP 通道給予路由器；對 Win2000/XP 來說，請使用 Network and Dial-up connections 或是 Smart VPN Client 等軟體幫忙建立 PPTP、L2TP 和 L2TP over IPSec 通道，您可以在包裝的光碟片中找到此軟體或是進入 http://www.draytek.com/ 網站下載中心取得，依照螢幕指示來安裝即可。

2. 在安裝成功之後，對於第一次使用的用戶，必須先按 **Step 0** 中的 **Configure** 按鈕，重新啓動主機。



3. 在 **Step 2. Connect to VPN Server** 中，按下 **Insert** 按鈕新增一個新的入口。

如果選擇的服務項目是 ***IPSec Tunnel***，如下圖所示：

Dial To VPN

Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : ********

Type of VPN

PPTP　L2TP

IPSec Tunnel　L2TP over IPSec

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Use default gateway on remote network

OK　Cancel

您可以進一步指定取得 IP、安全防護以及驗證的方法。若已選擇 Pre-Shared Key，那麼此設定必須與 VPN 路由器中的設定一致。

IPSec Policy Setting

My IP : 172.16.3.100

Type of IPSec

Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

Virture IP　DrayTek Virture Interface

Obtain an IP address automatically (DHCP over IPSec)

Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

Medium(AH)　High(ESP)

MD5　DES

Authority Method

Pre-shared Key : ******

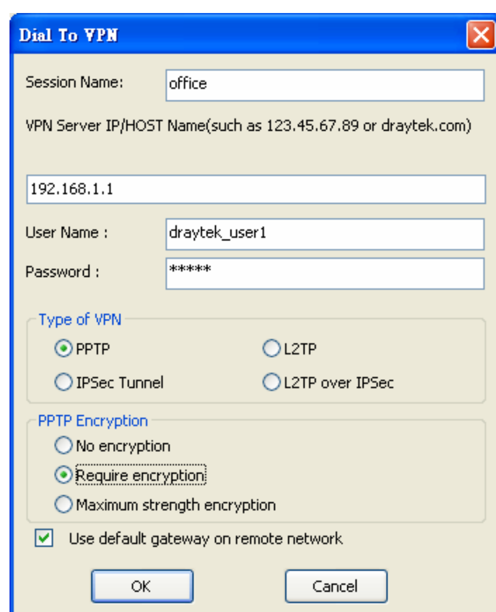
Certification Authority:

Browse...

OK　Cancel

如果選擇的是 PPP 為主的服務項目，您可以進一步指定 VPN 伺服器 IP 位址、使用者名稱、密碼和加密方法，使用者名稱和密碼必須和您在 VPN 路由器中所設定的內容一致。如欲使用遠端網路上預設的閘道，表示所有遠端主機上的封包都將會導引至 VPN 伺服器，然後再轉送到網際網路上，這樣會讓遠端主機看起來像是

在企業網路上運作一般。



4. 按 **Connect** 按鈕建立連線，當連線成功之時，您可以在右下方角落發現到綠色閃燈。

4.3 QoS 設定範例

假定電信工作人員有時在家中工作並且需要照料小孩，在工作時間，工作人員可使用家中的路由器，透過 HTTPS 或是 VPN 連接上總部的伺服器，來檢查電子郵件並存取公司內部的資料庫訊息，同時，小朋友也可以在休息室透過 Skype 彼此交談。

1. 進入**頻寬管理**之**服務品質**頁面。

頻寬管理 >> 服務品質(QoS)

基本設定

索引	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	
WAN1	啟用	10000Kbps/10000Kbps	上傳	25%	25%	25%	25%	不啟用	設定
WAN2	啟用	10000Kbps/10000Kbps	上傳	25%	25%	25%	25%	不啟用	設定

類別規則

索引	名稱	規則	服務類型
類別 1		編輯	編輯
類別 2		編輯	
類別 3		編輯	

2. 按WAN1 的**設定**連結，請確定左上角的**啓用服務品質(QoS)控制功能**已經勾選，選擇**雙向**作爲方向。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

☑ 啟用服務品質(QoS)控制功能 上傳

下載
上傳
雙向

WAN 下載頻寬

WAN 上傳頻寬

3. 回至上一層，按類別 1 的**編輯**連結以輸入索引類別 1 的名稱 **"E-mail"**，再按**確定**。

頻寬管理 >> 服務品質

類別索引#1

名稱 E-mail

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 ○	啟用	任何一種	任何一種	ANY	ANY

新增 編輯 刪除

確定 取消

4. 使用者可設定保留頻寬(例如 25%) 給予透過POP3 和SMTP通訊協定來傳送的電子郵件。參考下圖。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

☑ 啟用服務品質(QoS)控制功能 上傳

WAN 下載頻寬 10000 Kbps

WAN 上傳頻寬 10000 Kbps

索引	類別名稱	保留頻寬比例
類別 1		25 %
類別 2		25 %
類別 3		25 %
	其他	25 %

☐ 啟用 UDP 頻寬控制　　頻寬限制比率 25 %

連線狀態統計

確定 清除 取消

5. 回至上一層，按類別 2 的**編輯**連結以輸入索引類別 2 的名稱，於此索引中我們可以設定保留頻寬(例如 25%)給予**HTTP**。

頻寬管理 >> 服務品質(QoS)

基本設定

索引	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	
WAN1	啟用	10000Kbps/10000Kbps	上傳	25%	25%	25%	25%	不啟用	設定
WAN2	啟用	10000Kbps/10000Kbps	上傳	25%	25%	25%	25%	不啟用	設定

類別規則

索引	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

6. 選擇WAN1 的設定連結。
7. 勾選啟用**UDP頻寬控制**防止VoIP大量的UDP資料影響其他的應用程式。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

☑ 啟用服務品質(QoS)控制功能 上傳

WAN 下載頻寬 10000 Kbps

WAN 上傳頻寬 10000 Kbps

索引編號	類別名稱	保留頻寬比例
類別 1	E-mail	25 %
類別 2	HTTP	25 %
類別 3		25 %
	其他	25 %

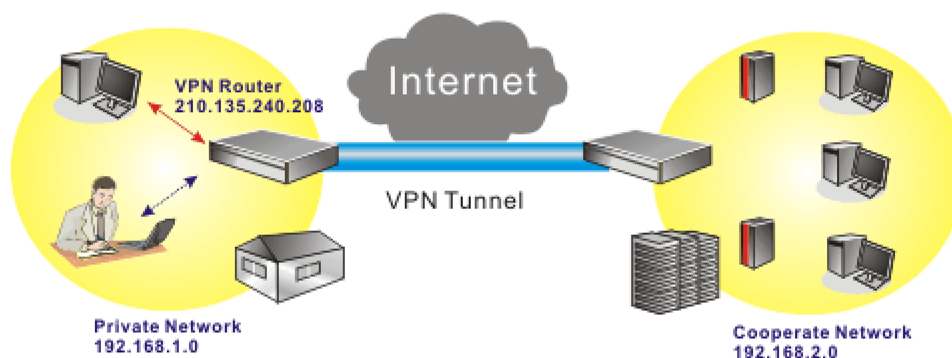
☑ 啟用 UDP 頻寬控制

頻寬限制比率 25 %

連線狀態統計

確定 清除 取消

8. 如果工作人員利用主機對主機的VPN通道，連上了總公司，(詳細設定請參考**VPN**一節)他可能已設定了相關的內容，請輸入索引編號 3 的類別名稱，在此類別中，工作人員將可完成一條VPN通道的保留頻寬設定。



9. 按**新增**以開啓新的視窗。

頻寬管理 >> 服務品質

類別索引#1

名稱 E-mail

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 ○	啟用	任何一種	任何一種	ANY	ANY

新增 編輯 刪除

確定 取消

10. 首先請勾選**啓用**方塊，接著按下**本機地址**的**編輯**按鈕以設定工作人員的子網路位址，按**遠端位址**的**編輯**按鈕設定總公司的子網路位址，其他的區域則不變，然後按下**確定**。

頻寬管理 >> 服務品質

編輯規則

☑ 啟用

本機地址 Any 編輯

遠端位址 Any 編輯

DiffServ CodePoint ANY

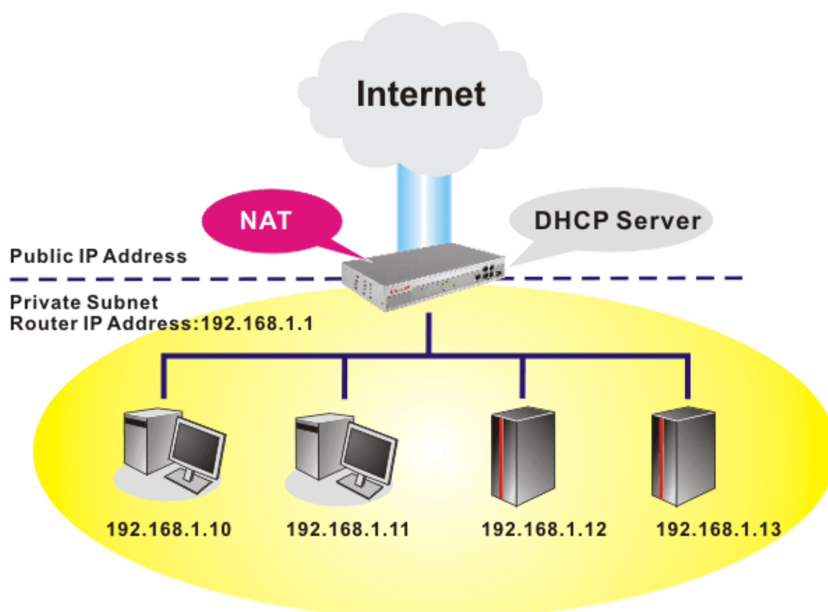
服務類型 ANY

附註: 請先選擇/設定 **服務類型**！

確定 取消

4.4 使用 NAT 來建立區域連線

預設設定和相關應用範例顯示如下，預設路由器之虛擬 IP 位址/子網路遮罩爲 192.168.1.1/255.255.255.0，內建之 DHCP 伺服器已經啓用，因此指定每個 NAT 的主機一個 192.168.1.x 的 IP 位址，範圍從 192.168.1.10 開始。



下圖爲區域網路的基本設定頁面，請適當調整，以符合 NAT 用途的需求。

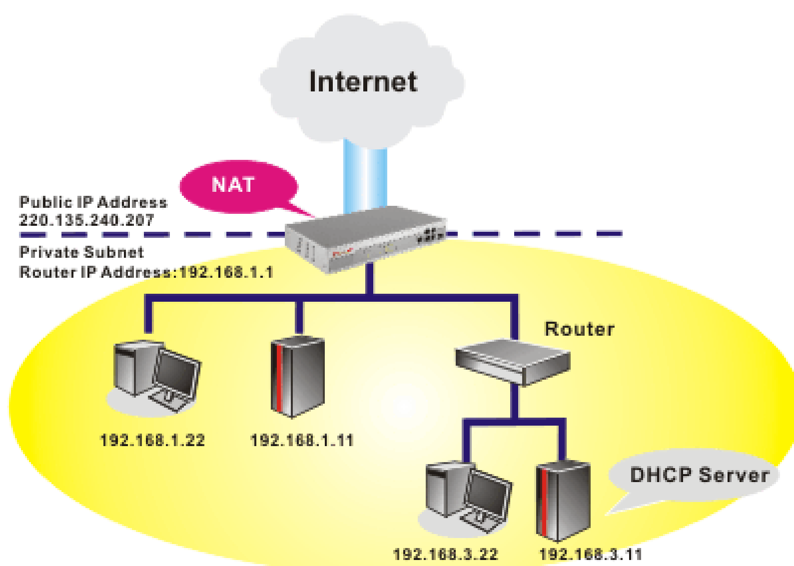
區域網路 >> 基本設定

區域網路 TCP / IP與 DHCP 設定

區域網路 IP 網路組態		DHCP 伺服器組態	
供 NAT 使用		◉啟用 ○停用	
第一 IP 位址	192.168.1.1	DHCP 中繼代理位址 ○第一子網路 ○第二子網路	
第一子網路遮罩	255.255.255.0	起始 IP 位址	192.168.1.10
供 IP 路由使用 ○ 啟用 ◉ 停用		IP 配置數量	50
第二 IP 位址	192.168.2.1	閘道 IP 位址	192.168.1.1
第二子網路遮罩	255.255.255.0	中繼代理程式IP位址	
	第二子網路 DHCP 伺服器	DNS 伺服器 IP 位址	
		☐ 使用 DNS 手動設定	
RIP 協定控制	停用	主要 IP 位址	
		次要 IP 位址	

確定

如要使用網路中的 DHCP 伺服器而非路由器內建的伺服器，您必須變更設定，如下所示：



下圖為區域網路的基本設定頁面，請適當調整，以符合 NAT 用途的需求。

區域網路 >> 基本設定

區域網路 TCP / IP與 DHCP 設定

區域網路 IP 網路組態

供 NAT 使用

第一 IP 位址 192.168.1.1

第一子網路遮罩 255.255.255.0

供 IP 路由使用 ◯ 啟用 ⦿ 停用

第二 IP 位址 192.168.2.1

第二子網路遮罩 255.255.255.0

[第二子網路 DHCP 伺服器]

RIP 協定控制 停用

DHCP 伺服器組態

◯ 啟用 ⦿ 停用

DHCP 中繼代理位址 ◯ 第一子網路 ◯ 第二子網路

起始 IP 位址 192.168.1.10

IP 配置數量 50

閘道 IP 位址 192.168.3.11

中繼代理程式IP位址

DNS 伺服器 IP 位址

☑ 使用 DNS 手動設定

主要 IP 位址 10.0.0.150

次要 IP 位址

[確定]

4.5 更新路由器韌體

更新韌體之前，您必須先安裝路由器工具，**Firmware Upgrade Utility** 即包含在 CD 中。

1. 將光碟片放進光碟槽中。
2. 請自網頁中，找出**工具程式**選單並點選進入頁面。
3. 在**工具程式**網頁上，按 **Install Now!** (位於 Syslog 說明下方) 以安裝相關程式。

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514



4. **RTSxxx.exe** 檔案將會複製到您的電腦上，請記住執行檔的儲存位置。
5. 進入 **www.draytek.com.tw** 網站，以尋找目前該路由器最新的韌體檔案。
6. 進入**支援服務 >> 檔案下載**，找到路由器機型名稱之後，選取其相關的韌體連結 **Vigor router** 的工具畫面將出現如下：

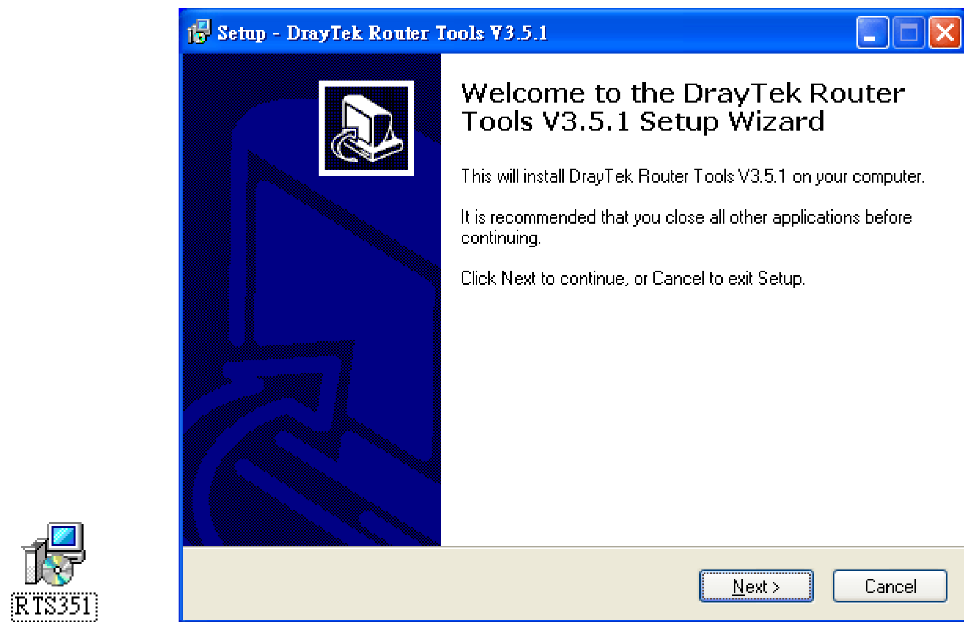
附註：

各產品的韌體不盡相同，錯誤的韌體將導致產品運作發生問題，以下我們已依據產品別分類，請依據您所購買的產品選擇適用之韌體下載。

工具名稱	更新日期	版本	作業系統	支援產品	下載
Router Tools	95 年 10 月 23 日	3.5.1	MS-Windows	全系列產品	zip
Smart VPN Client	95 年 8 月 18 日	3.2.6	MS-Windows	全系列產品	zip
LPR	94 年 6 月 27 日	1.0	MS-Windows	有Print 功能之產品	zip
VTA	94 年 9 月 15 日	2.8	Windows2000/XP	ISDN 產品	zip
DialPlan	95 年 1 月 26 日	2.5_lite	MS-Windows	VoIP 產品	zip

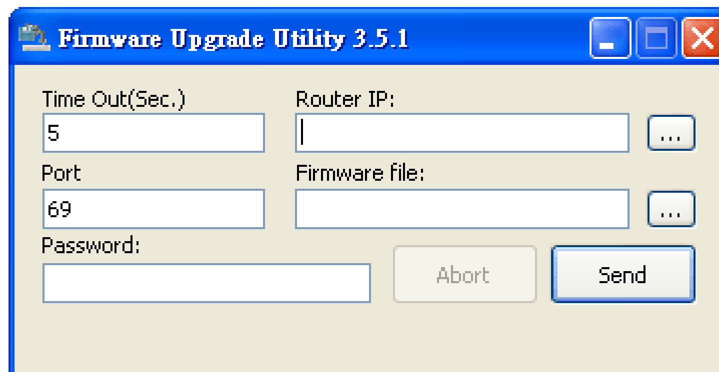
7. 插入路由器的 CD，請至相關連結處下載正確的韌體檔案(zip 檔案)。
8. 接著，解壓縮 ZIP 檔案。

9. 在路由器工具圖示上按二下，安裝精靈將出現如下：



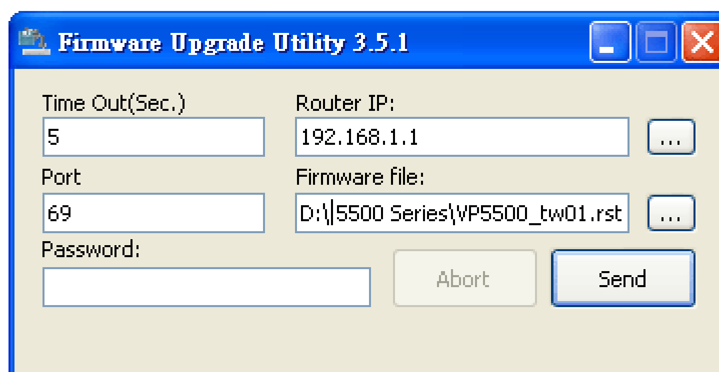
10. 依照螢幕指示安裝此工具，按下 **Finish** 以結束安裝。

11. 自開始選單中，指向程式集，然後選擇 **Router Tools XXX** >> **Firmware Upgrade Utility**。

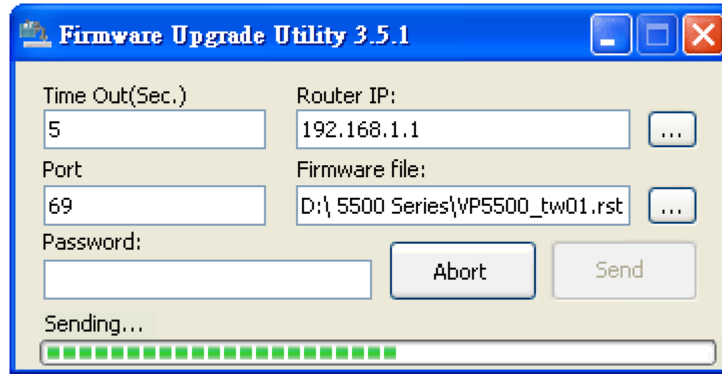


12. 輸入路由器 IP 地址，通常為 **192.168.1.1**。

13. 按韌體檔案(Firmware file)輸入欄右邊的按鈕，尋找您自公司網站下載之韌體檔案，您會看見二個副檔名不同的檔案：**xxxx.all** (可保持用戶原先的設定)以及 **xxxx.rst** (將用戶設定重新回復預設值)，請按照實際需要選擇任何一個。

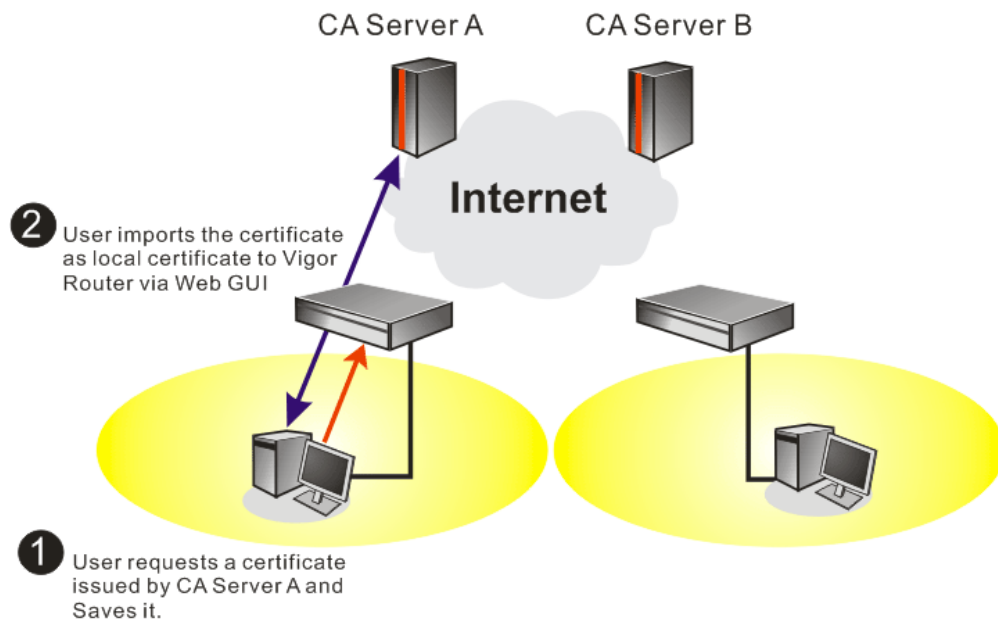


14. 按下 **Send**。



15. 現在韌體更新已完成。

4.6 在 Windows CA 伺服器上提出憑證需求



1. 選擇憑證管理>>本機憑證。按產生進入設定頁面。

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主體	狀態	編輯
本機	---	---	檢視 刪除

產生 匯入 頁面更新

X509 本機憑證

2. 請輸入憑證所需的相關資料，按畫面上的**產生**按鈕開始編輯憑證需求。

憑證管理 >> 本機憑證

產生憑證需求

主體替代名稱	
類型	IP 位址
IP	
主體名稱	
國家	
省份	
居住地區	
組織	
組織單位	
常用名稱	
電子郵件	
金鑰類型	RSA
金鑰大小	1024 Bit

產生

3. 複製並儲存 X509 本機憑證需求，稍後將會應用到此文字檔。

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主題	狀態	編輯
本機	/C=TW/O=Draytek/emailAddress...	Requesting	檢視 刪除

產生 匯入 頁面更新

X509 本機憑證設定需求


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYXl0ZWsxIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYBlce5OERSDfWknIdHblolkt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7evl87twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQAuSBRUGt4WlhH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86Ro08Jx0I45560xCZ/NlGh9VQ9Il
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```


4. 透過網頁瀏覽器連接 CA 伺服器，依照螢幕指示完成需求設定。下圖我們以 Windows 2000 CA 伺服器為範本，請選擇 **Request a Certificate**。

Microsoft Certificate Services -- vigor　　Home

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- ○ Retrieve the CA certificate or certificate revocation list
- ◉ Request a certificate
- ○ Check on a pending certificate

Next >

選擇 **Advanced request**，然後按 **Next**。

Microsoft Certificate Services -- vigor **Home**

Choose Request Type

Please select the type of request you would like to make:

○ User certificate request:

User Certificate

◉ Advanced request

Next >

挑選 **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**，然後按 **Next**。

Microsoft Certificate Services -- vigor **Home**

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

◉ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

匯入 X509 本機憑證文字檔，選擇 **Router (Offline request)** 或 **PSec (Offline request)** 。

Microsoft Certificate Services -- vigor **Home**

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t
A4GNADCBiQKBgQDQYB7wmZFfFhN9/IeQnG03Xk++
hX4bp89cUF9d1oACGGiM/tcBOckdcZdPFFvIXcP3
x/GOA7CTvO/fQzpxroCw1JTjLSjS0/Bn9v50951G

Browse for a file to insert.

Certificate Template:

Administrator

Administrator
Authenticated Session
Basic EFS
EFS Recovery Agent
User
IPSEC (Offline request)
Router (Offline request)
Subordinate Certification Authority
Web Server

Additional Attribut

Attributes:

Submit >

需求提出後，伺服器會給您一個憑證，請選擇 **ase 64 encoded** 憑證及下載該憑證，現在您應該會從伺服器取得一個憑證，請儲存該憑證。

5. 回到路由器畫面，進入**本機憑證**，按下**匯入**按鈕並瀏覽檔案以匯入憑證至路由器中。當您完成這個動作時，請按頁面更新，您就可以看見如下的視窗。

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主題	狀態	編輯
本機	/C=TW/O=Draytek/emailAddress...	Requesting	檢視 刪除

產生 匯入 頁面更新

X509 本機憑證設定需求


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYXl0ZWsxIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYXl0ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYBlce5OERSDfWknIdHblolkt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7evl87twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQAuSBRUGt4WlhH9N6/HwToem1tHQbcwjXvg/t7kFlzTJiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO8Jx0I4556OxCZ/NlGh9VQ9Il
I9FqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```

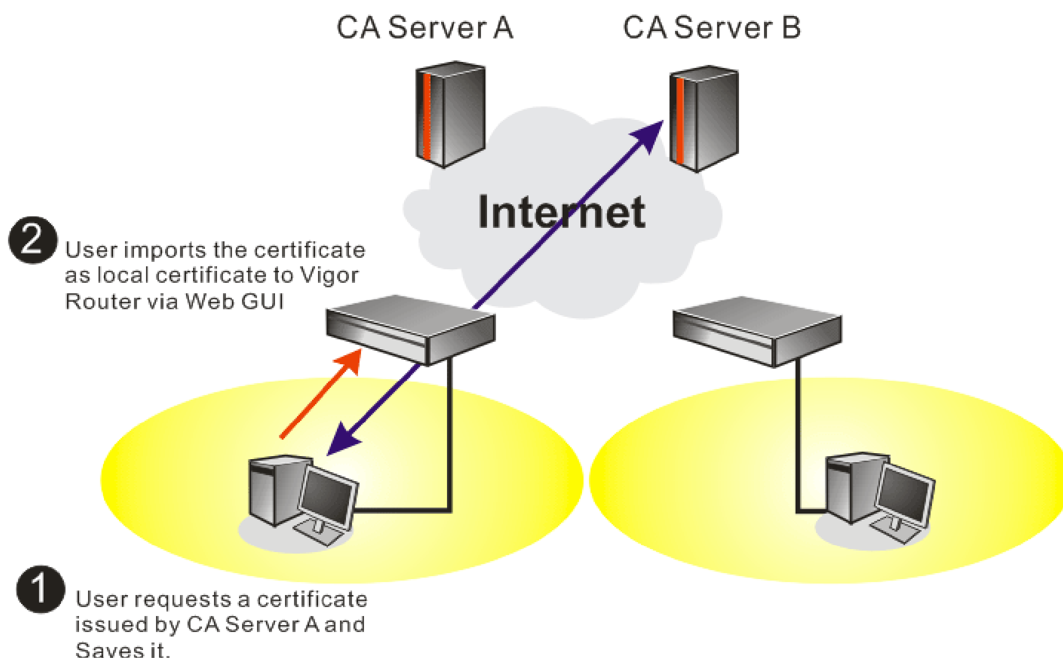

6. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

憑證需求資訊

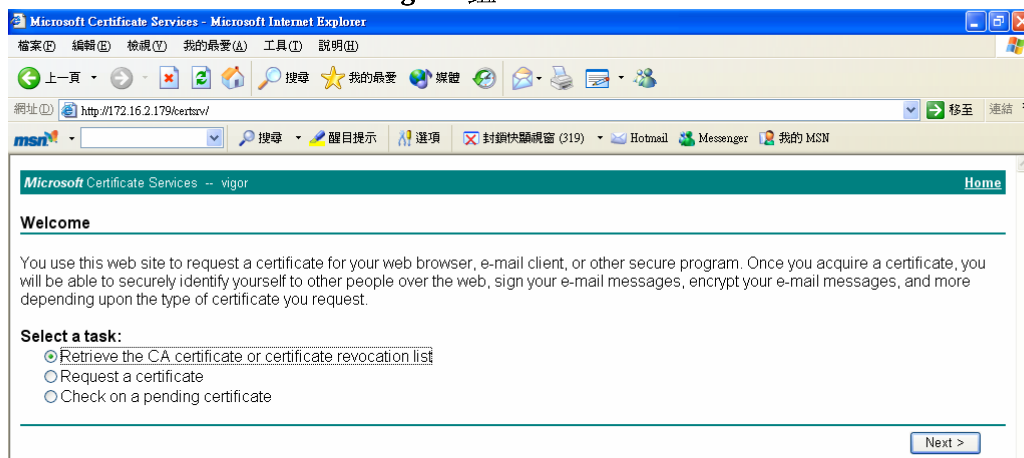
憑證名稱:	本機
發行者:	
主體:	/C=TW/O=Draytek/emailAddress=press@draytek.com
主體替代名稱:	DNS:draytek.com
有效期自:	
有效期到:	

關閉

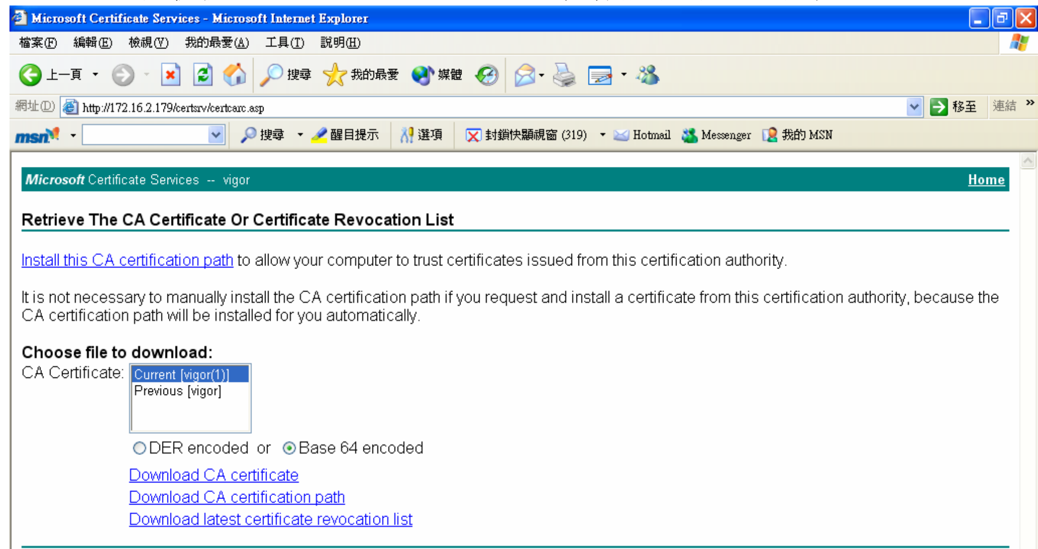
4.7 提出 CA 憑證要求並將之設定為 Windows CA 伺服器上具公信力之憑證



1. 使用瀏覽器連接至 CA 伺服器以取得您想要的憑證。按下 **Retrive the CA certificate or certificate recoring list** 鈕。



2. 在 **Choose file to download** 區中，按 CA Certificate **Current** 以及 **Base 64 encoded**，然後按 **Download CA certificate** 儲存該檔爲 cer. 檔案。



3. 回到路由器網頁設定畫面，進入**具公信力之 CA 憑證**，按**匯入**按鈕並瀏覽檔案以匯入憑證。當您完成這個動作之後，請按更新頁面察看最新的憑證使用狀況。

憑證管理 >> 具公信力之 CA 憑證

X509 具公信力之 CA 憑證設定

名稱	主體	狀態	編輯
Trusted CA-1	---	---	檢視 刪除
Trusted CA-2	---	---	檢視 刪除
Trusted CA-3	---	---	檢視 刪除

匯入　更新頁面

4. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

憑證詳細資訊

憑證名稱:	Trusted CA-1
發行者:	/C=US/CN=vigor
主體:	/C=US/CN=vigor
主體替代名稱:	DNS:draytek.com
有效期自:	Aug 30 23:08:43 2005 GMT
有效期到:	Aug 30 23:17:47 2007 GMT

關閉

> **注意:**在設定憑證之前，請先至**系統維護>>日期與時間**頁面中重新設定路由器的時間。

本頁留白供註解使用

5 疑難排解

這個章節將幫助您解決安裝完成路由器後，卻無法順利登入網際網路的情形。請依照以下的步驟檢查您路由器的基本設定。

- 檢查硬體狀態是否正常
- 檢查您個人電腦內的網路連線設定是否正確
- 從您的個人電腦 Ping 路由器是否正確
- 檢查你的 ISP 設定是否正確
- 必要時，請還原路由器出廠預設值

如果路由器的設完全正確但路由器仍舊無法正常運作，建議與購買的經銷商聯絡以協助您進行設定。

5.1 檢查硬體狀態是否正常

依照以下的步驟去確認路由器的硬體狀態。

1. 檢查電源線、區域網路(LAN)/無線區域網路(WLAN)電纜是否連線。詳細安裝資料，請參照 **2.1 硬體安裝**。
2. 開啓路由器後，確認 **ACT** 燈號是否為每秒閃動一次，並確認相對應的 **LAN** 燈號是否亮起。



3. 如果不是，表示硬體狀態在某些設定下發生錯誤，請回到 **2.1 硬體安裝**重新設定並再嘗試確認安裝無誤。

5.2 檢查您個人電腦內的網路連線設定是否正確

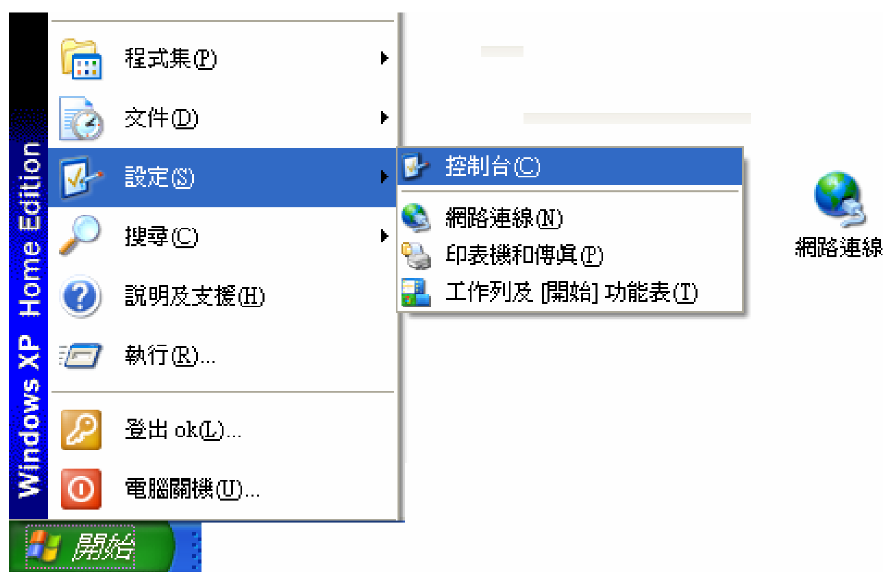
有時連線失敗的原因是在於網路連線設定錯誤。若在嘗試上述的步驟之後，網路連結依然失敗，請依照以下的步驟確定網路連線設定是否正常。

適用於 Windows



注意: 下列的範例是以 Windows XP 作業系統為基礎。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

1. 至**控制台**內，選擇**網路連線**並按滑鼠左鍵二下，進入網路連線畫面。



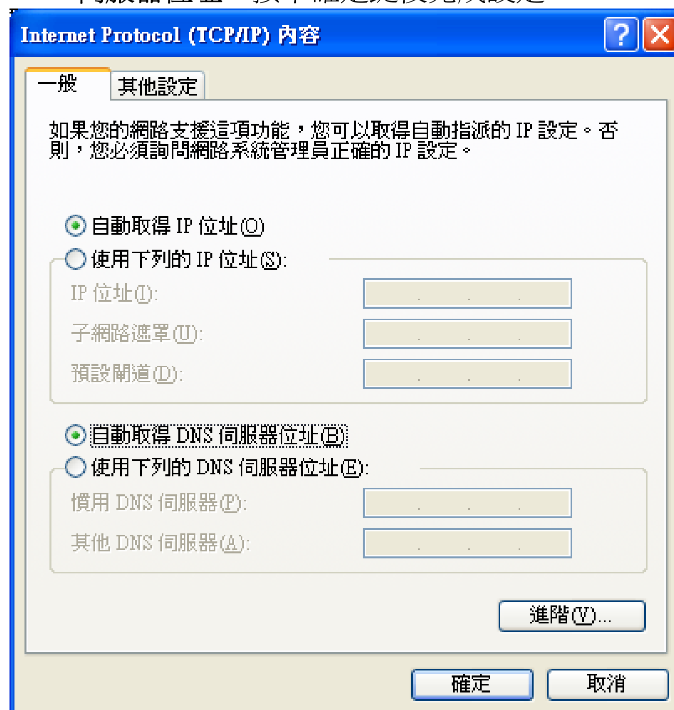
2. 選擇**區域連線**按滑鼠右鍵，選擇內容。



3. 進入區域連線內容畫面後，選擇 **Internet Protocol (TCP/IP)**，按下內容鍵。

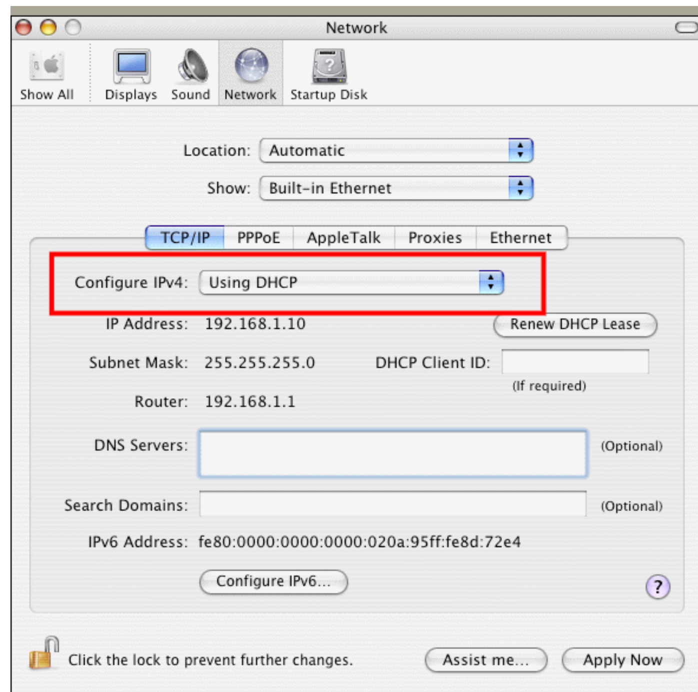


4. 進入 **Internet Protocol (TCP/IP)**內容畫面後，選擇自動取得 **IP** 位址及自動取得 **DNS** 伺服器位址，按下確定鍵後完成設定。



適用於 MacOs

1. 在桌面上選擇目前所使用的 MacOS 磁碟機，並按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 Network 檔案夾。
3. 進入 **Network** 畫面，在 Configure IPv4 選項中，選擇 **Using DHCP**。



5.3 從您的個人電腦 Ping 路由器是否正確

路由器的預設閘道為 192.168.1.1. 因為某些理由,你可能需要使用 " ping " 指令檢查路由器的連結狀態。重要在於電腦是否收到來自 192.168.1.1 的回應,如果沒有,請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定為自動取得 IP 位址。(請參照 6.2 檢查您個人電腦內的網路連線設定是否正確),請依照以下的步驟正確地 ping 路由器。

適用於 Windows

1. 開啓**命令提示字元視窗** (開始功能表選單 > 執行)。
2. 輸入 **command** (適用於 Windows 95/98/ME)或 **cmd** (適用於 Windows NT/ 2000/XP)。DOS 命令提示字元視窗將會出現。

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. 輸入 **ping 192.168.1.1** 並按下 **Enter**,如果連結成功,電腦會收到來自 192.168.1.1 的回應 **"Reply from 192.168.1.1: bytes=32 time<1ms TTL=255"** 。
4. 如果連結失敗(該行並未出現),請確認個人電腦的 IP 位址設定是否有誤。

適用於 MacOs (終端機)

1. 在桌面上選擇目前所使用的 MacOS 磁碟機,並按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**;終端機的視窗將會跳出顯現在螢幕。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常,終端機視窗會出現**"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms"** 的訊息。

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

5.4 檢查你的 ISP 設定是否正確

從網頁設定介面上，進入 **WAN>>網際網路連線**以檢查 ISP 設定。

按 WAN1/WAN2 的**細節設定**檢查先前所做的設定。

WAN >> 網際網路連線

網際網路連線

索引編號	顯示名稱	實體模式	連線模式	
WAN1		乙太網路	固定或動態 IP	細節設定
WAN2		乙太網路	無	細節設定

連線模式

固定或動態 IP
無
PPPoE
固定或動態 IP
PPTP

適用於 ADSL 非固定制(PPPoE)

1. 檢查是否已選擇啓用選項。
2. 檢查使用者名稱與密碼是否已輸入 **ISP** 提供給您的正確資料。

WAN >> 網際網路連線

WAN 1

PPPoE 用戶端模式
◉啟用 ○停用

ISP 存取設定
使用者名稱 84005755@hinet.net
密碼 ●●●●●●●●●
索引號碼(1-15) 於 排程 設定:
=> , , ,

PPP/MP 設定
PPP 驗證 PAP 或 CHAP
閒置逾時 -1 秒
IP 位址指派方式 (IPCP) WAN IP別名
固定 IP: ○ 是 ◉ 否 (動態IP)
固定 IP 位址

◉ 預設 MAC 位址
○ 指定 MAC 位址
MAC 位址:
00 50 7F C0 2F F5

確定 取消

適用於 Cable/光纖/ADSL 固定制 (固定或動態 IP)

1. 檢查是否已選擇寬頻存取的啓用選項。

WAN >> 網際網路連線

WAN 1

固定或動態 IP (DHCP用戶端)
◉啟用 ○停用

維持 WAN 連線
☐ 啟用 PING 以保持常態連線
PING 到指定的 IP 位址
PING 間隔 0 分(s)

RIP 協定
☐ 啟用 RIP

WAN IP 網路設定 WAN IP 別名
○ 自動取得 IP 位址
路由器名稱 *
網域名稱 *
* : 有些 ISP 需要此項設定名稱

◉ 指定 IP 位址
IP 位址 172.16.3.229
子網路遮罩 255.255.255.0
閘道 IP 位址 172.16.3.1

◉ 預設 MAC 位址
○ 指定 MAC 位址
MAC 位址:
00 50 7F 00 00 01

DNS 伺服器 IP 位址
主要 IP 位址 10.0.0.150
次要 IP 位址

確定 取消

2. 如果您選擇了**指定 IP 位址**項目，請檢查 **IP** 位址、**子網路遮罩**與**閘道 IP** 位址是否設定正確(必須符合 ISP 提供給您的資料)。

5.5 還原路由器原廠預設組態

有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用**軟體重新設定**或**硬體重新設定**的方法還原路由器設定值。



警告：在使用原廠預設組態後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定，預設出廠的密碼為空白。

軟體重新設定

您可以利用 Web 介面將路由器的重置成原廠預設組態。

點選網頁左下方**系統管理**的**重啓系統**選項，選擇**使用原廠預設組態**，等待數秒以後，路由器將重新啓動並將所有設定還原成原廠預設組態。

系統維護 >> 重啟路由器

重啟路由器

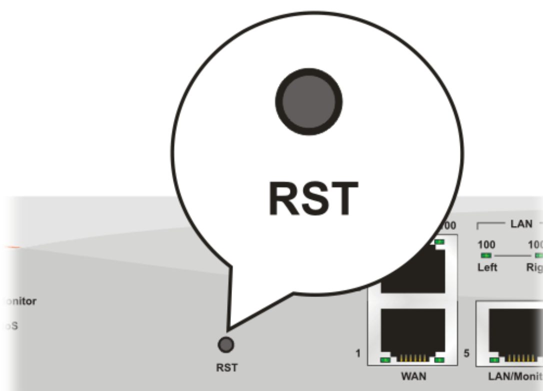
您想重新啟動路由器嗎？

◉ 使用目前組態
○ 使用原廠預設組態

[確定]

硬體重新設定

當路由器正在運作時（ACT 燈號閃爍），壓住 **RST** 鈕超過 5 秒，當您看到 ACT 燈號開始快速閃爍時，請鬆開 **RST** 按鈕，此時，路由器將會還原成原廠預設組態。



在恢復原廠預設組態後，您可以再次依照所需設定路由器。

5.6 聯絡您的經銷商

假如經過多次嘗試設定後，路由器仍舊無法正常運作，請立即與經銷商或與居易科技技術服務部聯絡 support@draytek.com。